U.S. Department of Transportation Federal Railroad Administration PNT Resiliency Pilot Program Report

Phase I Report

Melanie Soares, George Mantis, Stephen Mackey, Andrew Hansen, Hadi Wassaf, Christopher Scarpone, Jonathon Poage, Robert Samiljan, John Flake

Final Report — April 2025

DOT-VNTSC- OST-25-05

Prepared for:
Office of the Assistant Secretary for Research and Technology (OST-R)
Office of PNT and Spectrum Management
1200 New Jersey Avenue, SE
Washington, DC 20590

U.S. Department of Transportation
Volpe Center

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 18-04-2025	**2. REPORT TYPE**	**3. DATES COVERED *(From - To)*** 17-10-2022 – 30-06-2025

4. TITLE AND SUBTITLE

U.S. Department of Transportation | Federal Railroad Administration

PNT Resiliency Pilot Program Report | Phase I Report

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Melanie Soares, George Mantis, Stephen Mackey, Andrew Hansen, Hadi Wassaf, Jonathan Poage, Christopher Scarpone, Robert Samiljan, John Flake

5d. PROJECT NUMBER
51OS92AB22

5e. TASK NUMBER
ABQ723

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Department of Transportation
John A Volpe National Transportation Systems Center
220 Binney Street
Cambridge, MA 02142

8. PERFORMING ORGANIZATION REPORT NUMBER
DOT-VNTSC-OST-25-05

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of the Assistant Secretary of Transportation for Research and Technology (OST-R)
Office of Positioning, Navigation and Timing (PNT) and Spectrum Management
U.S. Department of Transportation
1200 New Jersey Avenue, SE, Washington, DC 20590

10. SPONSOR/MONITOR'S ACRONYM(S)
OST-R

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

This report contains Controlled Unclassified Information and is not for Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In order to improve the resilience of the Nation's critical infrastructure to GPS disruptions, the President issued Executive Order (EO) 13905 "Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services," in February 2020 to foster responsible use of PNT services. In accordance with Section 4(g) of EO 13905, the U.S. Department of Transportation (USDOT) undertooka Pilot Program to develop critical infrastructure profiles for the transportationsector. The Department's focus encompasses GPS jamming and spoofing in the rail mode, through a partnership between the Office of the Assistant Secretary for Research and Technology (OST-R) and the Federal Rail Administration (FRA), as its next candidate for PNT Profile development.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF: Unclassified			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** George Mantis
a. REPORT	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	none	126	**19b. TELEPHONE NUMBER *(include area code)*** 617-494-2732

SI* (MODERN METRIC) CONVERSION FACTORS

APPROXIMATE CONVERSIONS TO SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
		LENGTH		
in	inches	25.4	millimeters	mm
ft	feet	0.305	meters	m
yd	yards	0.914	meters	m
mi	miles	1.61	kilometers	km
		AREA		
in^2	square inches	645.2	square millimeters	mm^2
ft^2	square feet	0.093	square meters	m^2
yd^2	square yard	0.836	square meters	m^2
ac	acres	0.405	hectares	ha
mi^2	square miles	2.59	square kilometers	km^2
		VOLUME		
fl oz	fluid ounces	29.57	milliliters	mL
gal	gallons	3.785	liters	L
ft^3	cubic feet	0.028	cubic meters	m^3
yd^3	cubic yards	0.765	cubic meters	m^3
		NOTE: volumes greater than 1000 L shall be shown in m^3		
		MASS		
oz	ounces	28.35	grams	g
lb	pounds	0.454	kilograms	kg
T	short tons (2000 lb)	0.907	megagrams (or "metric ton")	Mg (or "t")
oz	ounces	28.35	grams	g
		TEMPERATURE (exact degrees)		
°F	Fahrenheit	5 (F-32)/9 or (F-32)/1.8	Celsius	°C
		ILLUMINATION		
fc	foot-candles	10.76	lux	lx
fl	foot-Lamberts	3.426	candela/m^2	cd/m^2
		FORCE and PRESSURE or STRESS		
lbf	poundforce	4.45	newtons	N
lbf/in^2	poundforce per square inch	6.89	kilopascals	kPa

APPROXIMATE CONVERSIONS FROM SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
		LENGTH		
mm	millimeters	0.039	inches	in
m	meters	3.28	feet	ft
m	meters	1.09	yards	yd
km	kilometers	0.621	miles	mi
		AREA		
mm^2	square millimeters	0.0016	square inches	in^2
m^2	square meters	10.764	square feet	ft^2
m^2	square meters	1.195	square yards	yd^2
ha	hectares	2.47	acres	ac
km^2	square kilometers	0.386	square miles	mi^2
		VOLUME		
mL	milliliters	0.034	fluid ounces	fl oz
L	liters	0.264	gallons	gal
m^3	cubic meters	35.314	cubic feet	ft^3
m^3	cubic meters	1.307	cubic yards	yd^3
mL	milliliters	0.034	fluid ounces	fl oz
		MASS		
g	grams	0.035	ounces	oz
kg	kilograms	2.202	pounds	lb
Mg (or "t")	megagrams (or "metric ton")	1.103	short tons (2000 lb)	T
g	grams	0.035	ounces	oz
		TEMPERATURE (exact degrees)		
°C	Celsius	1.8C+32	Fahrenheit	°F
		ILLUMINATION		
lx	lux	0.0929	foot-candles	fc
cd/m^2	candela/m^2	0.2919	foot-Lamberts	fl
		FORCE and PRESSURE or STRESS		
N	newtons	0.225	poundforce	lbf
kPa	Kilopascals	0.145	poundforce per square inch	lbf/in^2

*SI is the symbol for the International System of Units. Appropriate rounding should be made to comply with Section 4 of ASTM E380. (Revised March 2003)

Acknowledgments

The authors wish to thank

- US DOT OST-R: Karen Van Dyke
- US DOT FRA: Matt Brewer, Andrew Straatveit, Tyrone Clements, Mike Drury
- Amtrak: Eileen Reilly, Walter Stadtlander

Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Term
3D	Three dimensional
ACSES	Advanced Civil Speed Enforcement System
AGC	Automatic gain control
CPNT	Complementary positioning, navigation, and timing
CRPA	Controlled reception pattern antenna
CRUCIBLE	Federal data repository of suspected cases of GNSS purposeful interference
CSF	Cybersecurity framework
DHS	Department of Homeland Security
DOD	Department of Defense
ECDIS	Electronic chart and information display system
EO	Executive Order
FRA	Federal Railroad Administration
GAJT	GPS Anti-Jam Antenna Technology
GET-CI	GPS Equipment Testing for Critical Infrastructure
GLONASS	GLObal NAvigation Satellite System
GNSS	Global navigation satellite system
GPS	Global Positioning System
I-ETMS	Interoperable Electronic Train Management System
IMU	Inertial measurement unit
LEO	Low Earth orbit
MARAD	Maritime Administration
MSC	Military Sealift Command
MRPA	Modified Reception Pattern Antenna
NEC	Northeast Corridor
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Internal Report
NIWC	Naval Information Warfare Center
OA	Operating Administration of DOT
OST-R	Office of the Assistant Secretary of Transportation for Research and Technology
PNM	Precision Navigation Module
PNT	Positioning, Navigation and Timing
PPP	Precise Point Positioning
PSD	Power Spectral Density
PTC	Positive Train Control
RF	Radio frequency
RRF	Ready Reserve Force

Abbreviation	Term
SBAS	Satellite-based augmentation system
SS	Steam ship
STL	Satellite time and location
TPOI(s)	Track Point(s) of Interest
TRL	Technology Readiness Level
USDOT	U.S. Department of Transportation
UTC	Coordinated Universal Time

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary

The Role of GPS in Transportation

The U.S. Global Positioning System (GPS) was originally developed by the U.S. Department of Defense to improve en route navigation and positioning for military purposes. The first GPS satellites were launched in 1978, with the full 24-satellite constellation declared operational in April 1995. The "selective availability" feature—which intentionally degraded the quality of the GPS signal available to civilian users world-wide by introducing errors of 50 to 100 meters—was turned off in 2000, increasing the precision of GPS position and opening the door to its widespread adoption for civilian positioning, navigation, and timing (PNT) applications globally.

Although conceived as a military PNT system, the potential of GPS for civilian applications became immediately apparent. The first commercially available GPS receiver was introduced in 1981. At nearly 59 pounds, it was hardly "portable," took nearly 20 minutes to initially acquire a position, and cost over $119,000, putting it out of reach of most users. Subsequent advances in miniaturization of GPS receiver technology, along with a revolution in the development of computer-based geographic information system (GIS) applications—whether mapping, surveying, routing, fleet management, asset recovery, or package tracking—encouraged innovation, spurred growth, and opened new markets beyond basic point-to-point navigation.

Today, GPS has become the ubiquitous global navigation satellite system (GNSS), and the gold standard for PNT services both in the U.S. and globally. It is used across all transportation modes—aviation, maritime, surface, rail, even pipelines—to improve the safety and efficiency of the U.S. National Transportation System. However, with that ubiquitous dependence comes both greater risk and greater consequence should the GPS signal be disrupted or degraded, whether intentionally or unintentionally.

The U.S. Department of Transportation PNT Profile Pilot Program

The need to address the vulnerability of GPS is recognized quite early on and has been a topic of continuous focus across multiple administrations. In a latest series of coordinated efforts, in order to improve the resilience of the Nation's critical infrastructure to GPS disruptions, the President issued Executive Order (EO) 13905 "Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services," in February 2020 to foster responsible use of PNT services. In accordance with Section 4(g) of EO 13905, the U.S. Department of Transportation (U.S.DOT) undertook a PNT Pilot Program to develop critical infrastructure profiles for the transportation sector. The Department initially focused on GPS jamming and spoofing in the maritime environment, and later turned to the rail sector via a partnership between the Office of the Assistant Secretary for Research and Technology (OST-R) and the Federal Railroad Administration (FRA). FRA is responsible for the safety standards governing U.S. freight and passenger rail operations. Trains and rail networks rely on GPS receivers and other PNT data for reliable positioning and timing, and safe navigation along train tracks. Further consideration of the applicability of EO 13905 led to the addition of Amtrak as a project partner, with its passenger rail service providing the use case for this project.

The Pilot Program sought to raise awareness of the extent to which rail depends on PNT services; identify approaches for rail operations to withstand disruption or manipulation of those services; and to engage the community of rail operators to promote the responsible use of PNT services. In August 2023, U.S. DOT met with industry and government representatives at their respective rail test facilities in Pueblo, CO. The objective of these site visits was to raise awareness of the impact of EO 13905 on rail operations as well as learn current dependencies on PNT services among freight rail operators, regulators, enforcement organizations, technology providers, PNT experts, and policy agencies. In November 2023, the Volpe National Transportation Systems Center (Volpe Center, a part of the U.S. DOT) began work supporting the rail PNT Pilot Program, through an inter-agency agreement with OST-R.

Addressing the specifics of the rail sector, the Volpe team conducted an industry survey and literature search, with guidance from FRA and Amtrak, to identify GNSS receivers and antennas of interest. Information was also gathered in this fashion on current and future Complementary Positioning, Navigation and Timing (CPNT) sources, that is, PNT other than GPS. Following the information gathering process, the Program team coordinated technical data-collection efforts at a major U.S. Government jamming and spoofing event to address detailed identification of vulnerabilities, assess threats, and consider complementary and backup PNT services that could serve as mitigations to operational impacts.

The Wabtec GoLinc™ Precision Navigation Module (PNM) was selected as the rail-representative PNT receiver. This unit, under testing and consideration by multple providers in the U.S. freight rail industry, is of interest and relevance to Amtrak. A number of GNSS antennas were selected to be paired with the GoLinc™ receiver, two protected and two unprotected. The unprotected antennas were the Sinclair™ SM714, currently in use by Amtrak, and the Tallysman™ TW3972XF, widely used by the freight rail industry. The NovAtel™ GAJT-4 CRPA and GPSSource™ MRPA comprised the protective solutions.

The above equipment was tested at NAVFEST 2024. NAVFEST is a U.S. Government active jamming and spoofing event conducted periodically at the U.S. Army's White Sands Missile Range in New Mexico. The 2024 test event lasted two weeks and included static and dynamic jamming and spoofing scenarios. Each week the GoLinc PNMs were paired with one protected antenna and one unprotected antenna. A change of antennas between the two weeks allowed testing the PNMs with a total of four antennas.

During NAVFEST 2024, the equipment under test demonstrated a relative overall order of device performance under a variety of spoofing and jamming conditions, though exceptions occasionally occurred for certain performance criteria in certain scenarios. Protected technologies (Modified

Reception Pattern Antenna (MRPA), and GPS Anti-Jam Antenna Technology (GAJT)) typically showed favorable performance over the unprotected technologies (Sinclair, Tallysman). This is consistent with expectations based on the level of sophistication of the protection technologies; for example, a multi-element CRPA is expected to provide greater protection than a single-element MRPA.

The Wabtec GoLinc PNM yielded lower horizontal position errors overall with a tighter spread compared to an alternative receiver (one utilized for another program) while obtaining static reference data. This indicates superior baseline performance for the Wabtec GoLinc PNM receiver. Signal availability indicated an overall relative order of performance favoring the protected antennas (MRPA, GAJT) which outperformed the unprotected technologies (Sinclair, Tallysman). The same holds true when assessing static response. Regarding static recovery, overall each receiver-antenna pair demonstrated subtle differences in the distributions of time to recover without any overwhelming advantages; however, the GoLinc-PNM Sinclair pairing experienced the most failures to recover, with twice as many failures as the GoLinc PNM-MRPA pairing.

Both freight rail operators and Amtrak have stated dead reckoning in GNSS-challenged environments as a primary PNT challenge.[1] Position initialization for a train beginning operation requires a valid GNSS signal, and while operating with GNSS coverage, a train may continue only a short distance after degradation or loss of the GPS signal. Rail operators seek to perform initialization without GNSS, and to extended dead reckoning operations (e.g. not stopping a train due to degraded GNSS before dead reckoning). Amtrak and the freight rail industry expressed interest in Machine Vision, Ground Penetrating Radar, and Ultra Wide Band technologies for improved dead reckoning operations. The fundamental basis for each candidate is locomotive-mounted front-end sensor data to determine train position relative to known track points of interest. While these technologies exist for other applications, such as track inspection, there exist several obstacles to their adoption as a real-time PNT source. Low Technology Readiness Level (TRL) in CPNT applications provides the greatest challenge for either technology; future work will address testing and maturation.

Pilot Project Findings and Recommendations

The FRA Pilot Program focused on GNSS equipment for passenger rail in the U.S. and provided findings and recommendations along each of the four components by:

1. Partnering with Amtrak as the use case for this program, through industry discussions and given the applicability of EO 13905 to the rail Mode.
2. Identifying specific passenger rail GNSS equipment through industry outreach and study of Amtrak trains.
3. Detecting the disruption and manipulation of GNSS service through successful testing of rail PNT

[1] Dead Reckoning is the process of calculating a train's current position based on the knowledge of the previous position and other parameters, such as speed, typically provided by an IMU.

equipment in “live sky” normal and disrupted/manipulated conditions. The primary evaluation in the study leveraged NAVFEST as the environment for testing identified GNSS equipment with and without added protective capability.

4. Identifying both existing and complementary PNT data sources that are suitable for passenger rail operations through industry outreach, literature search, and discussions with project partners.

The basis for the Pilot Program was the NIST Foundational PNT Profile specified in NISTIR 8323. As a Pilot Program, the team sought to develop actionable areas for increasing on-board rail PNT resilience. The central findings from the Program team were developed through the five NISTIR 8323 Framework Core functions. Addressing those five functions led to three actionable fronts for managing operational risk from PNT disruption and/or manipulation:

1. Know your risks;
2. Protect your systems; and
3. Incorporate diversified sources of PNT signals.

In alignment with the actionable objectives of the Pilot Program, the project’s findings are suitable for application in passenger rail service and should be considered as capabilities that can be incorporated into a system solution for satisfying GNSS resiliency requirements. The protective and diversifying solutions are effective and commercially available. The results provided in this report demonstrate that these solutions should be further evaluated with respect to the full set of operational requirements for a platform such as an Amtrak locomotive. However, from the PNT Profile perspective, the U.S. DOT Pilot Program findings lead to two recommendations for improving PNT resilience.

1. Protect existing or new GNSS equipment on passenger trains with controlled reception pattern antenna (CRPA) technology. Solutions such as the Hexagon GAJT-410MS can protect GPS-derived PNT outputs, with no further changes needed to on-board equipment. When paired with the GAJT nulling antenna, the GoLinc PNM receiver will be unable to demodulate the spoofing data therefore protecting the receiver from the vast majority of both signal and data spoofing attacks. This solution, if desired, does have the capability to serve also in a detect-and-characterize function (power and direction of arrival) on interfering signals. Further, a dual antenna/receiver pair can be used to detect a spoofing attack through self-differential means. (A concept under study by the industry proposes a GNSS antenna-receiver set installed at each end of a train and could potentially also furnish this spoofing attack detection capability.)
2. Augment GNSS with CPNT. Solutions such as Advanced Civil Speed Enforcement (ACSES) currently provide a complementary PNT source for train positioning. However, sensor fusion is not yet enabled on board passenger trains. Further, ACSES is limited to the Northeast Corridor (NEC) and is not deployable across the PTC systems of nationwide rail networks.

Given the current interest in the rail sector for CPNT technologies over augmentation of GNSS, the cost of a GNSS-protective solution is an additional consideration. Thus, a business case analysis must be made for investment in protective GNSS solutions vice PNT complementary technology investment.

1. Introduction

Background

The White House issued Executive Order (EO) 13905, "Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services," on February 12, 2020.[1] The goal of this initiative is to foster responsible use of positioning, navigation, and timing (PNT) services by critical infrastructure users, owners, and operators (including the transportation sector), thus strengthening national resilience. EO 13905 seeks to ensure that disruption or manipulation of PNT services does not undermine the reliability or efficiency of critical infrastructure services by:

- Raising awareness of the extent to which critical infrastructure depends on PNT services;
- Ensuring critical infrastructure can withstand disruption or manipulation of PNT services; and
- Engaging public and private sectors to promote responsible use of PNT services.

Section 4(g) of EO 13905 states, "Within 180 days of the date of this order, the Secretary of Transportation, Secretary of Energy, and Secretary of Homeland Security shall each develop plans to engage with critical infrastructure owners and operators to evaluate the responsible use of PNT services. Each pilot program shall be completed within 1 year of developing the plan, and the results shall be used to inform the development of the relevant PNT profile and research and development (R&D) opportunities." The initiative to develop PNT resiliency plans for transportation critical infrastructure is broadly organized with the U.S. Department of Transportation (U.S. DOT) as the "U.S. DOT PNT Pilot Program."

The Secretary of Transportation has overall leadership responsibility for civil PNT matters. Within the DOT, the Office of the Assistant Secretary of Research and Technology (OST-R) coordinates PNT initiatives and planning across all modes of transportation, including intermodal engagement. The Federal Railroad Administration (FRA) is the Operating Administration (OA) of DOT with responsibility for rail-borne transportation.[2] Its programs promote the use of rail networks, their integration with other modal segments of the National Transportation System, and to ensure the safe and efficient movement of passengers and freight via rail. FRA works across many areas encompassing issuance, implementation, and enforcement of safety regulations; managing Federal investments in freight and passenger rail across the country; and supporting research and technology development.[3]

The National Railroad Passenger Corporation, also known as Amtrak, is a Federally-chartered corporation, operated and managed as a for-profit company, but with the U.S. government as its majority shareholder. Amtrak operates intercity passenger rail services in 46 states and the District of Columbia, with connecting services in Canada and Mexico.[4] Congress created Amtrak through the Rail Passenger Service Act of 1970, whereby Amtrak assumed the common carrier obligations of privately-owned railroads in exchange for the right to priority access of their tracks for incremental cost. Amtrak's

Board of Directors includes the U.S. DOT Secretary or a designee thereof. FRA provides administration and oversight for Amtrak.[5] FRA oversees Amtrak's performance, inspects safety compliance, issues and administers grants, and provides technical assistance and standards.

OST-R identified the rail transportation mode as the next candidate for its U.S. DOT Pilot Program, which began with the Maritime Administration (MARAD). Working with FRA and the rail industry, Volpe refined the objective of this project with a focus on Amtrak passenger rail service. This initiative addresses Global Positioning System (GPS) interference that affects intercity passenger train service, while also considering complementary PNT technologies whose adoption could mitigate those impacts. Applicable results and lessons learned from the FRA Pilot Program will inform future FRA rulemaking and Amtrak service regarding PNT in rail operations. These will also be considered when addressing other modes of transportation (such as aviation, vehicles, and pipeline) to support PNT resiliency.

GPS Jamming and Spoofing

Accurate and reliable PNT capabilities are essential for safety in all modes of transportation including rail. The primary and most recognizable PNT service supporting critical infrastructure is GPS. However, because GPS relies upon signals broadcast from a space-based satellite constellation, its signals are low-power at the receiver and thus vulnerable to unintentional and intentional disruption. Natural and human-made features such as canyons and tunnels physically block the GPS signal, while background RF signals such as television and cellular may cause interference. Bad actors worldwide have performed intentional jamming and spoofing of GPS signals with impacts to commercial and civil air, marine, and surface transportation.

GPS signal jamming, whether intentional or unintentional in origin, is defined as a denial or degradation of GPS signal reception resulting from radio frequency interference. The term spoofing in GPS is much more nuanced and complex. Spoofing is caused by RF waveforms that mimic true signals in some ways, but deny, degrade, disrupt, or deceive a receiver's operation when they are processed. Spoofing may be unintentional, such as effects from the signals of a GPS repeater, or they may be intentional and even malicious. There are two classes of spoofing:

1. Measurement spoofing introduces RF waveforms that cause the target receiver to produce incorrect measurements of time of arrival or frequency of arrival or their rates of change; and
2. Data spoofing introduces incorrect data to the target receiver for its use in processing of signals and the calculation of PNT.

Either type of spoofing can cause a range of effects, from incorrect outputs of PNT to receiver malfunction. The onset of these effects can be instantaneous, intermittent, or delayed and it is possible for effects to continue even after the spoofing has ended.

Within the context of this report, we will be referring to, and evaluating equipment (both stand-alone as well as in combination with others) performance against, jamming and measurement spoofing. Since GPS receivers are designed to lock onto the strongest signals available, measurement spoofing occurs when a bogus GPS signal overpowers and replaces the authentic or intended GPS signal. This type of spoofing can be intermittent and subtle or obvious and extreme. For example, it may be easy to detect these spurious signals if a GPS receiver suddenly indicates a position hundreds of miles from where you were a few minutes ago or if there is a noticeable time shift. Alternatively, the spurious signals may only intermittently, and subtlety deviate from the authentic signal(s) so that the intended navigation shifts so slowly that the deviation is not noticed until the spoofing target is already off course. Since a higher power level signal is associated with both jamming and signal spoofing, the mitigating equipment tested in this evaluation is based on technology that detects power of arrival (PoA). Some devices also incorporate the ability to detect a pulsating signal and/or angle of arrival (AoA), which is necessary to identify the direction from which the spurious signal was transmitted. This capability allows for the unwanted signal(s) to be rejected and removed from the solution. However, even with these sophisticated capabilities and devices to enhance the resiliency of GPS, there are existing and emerging threats that can subvert these protective technologies.

Motivation for Rail

Rail systems throughout the world rely on GPS to track the movement of locomotives, rail cars, maintenance vehicles, and wayside equipment in real time.[6] Utilization of GPS provides synchronization for the timing of railroad communication systems (voice and data) between locomotive engineers and dispatchers, and intermodal communications among trains, rail stations, marine ports, and airports. GPS also enables the automation of faster, more accurate track surveying, mapping and inspection vice non-GPS-based systems, which saves time and money while improving safety.

A GPS anomaly in Denver, CO on January 21-22, 2022, provided an example of the impact of GPS disruptions for rail operations. A local RF emitter unintentionally transmitted a signal that interfered with GPS signal reception for a period of 33.5 hours.[7] This created widespread disruption of GPS signal reception in the Denver metropolitan area, resulting in degraded operations for rail and other critical infrastructure sectors. Specific impacts included interference in Positive Train Control (PTC) services in addition to the National Airspace System and Public Safety Land Mobile Radio. Network communications towers supporting PTC connectivity lost GPS timing at some receivers.[8]

PTC is the primary PNT dependency for rail. PTC utilizes data from a combination of GPS and on-board sensors to determine a train’s location relative to an on-board track database, and is described in detail in Appendix A. Through PTC, trains rely on PNT (GPS combined with one or more CPNT sources); disruptions force trains to stop, underscoring the criticality of PTC for the rail network. PTC not only impacts safety (a U.S. DOT priority), it also potentially enables cost savings through increased rail capacity and better allocation of resources for rail operators, though with added expense.

The National Transportation Safety Board (NTSB), through investigations into rail accidents, stated 22 incidents in which PTC problems were a contributing factor.[9] In single-train incidents with PTC-related causes, factors included derailments and collisions (not with other trains) due to incomplete PTC installations. In PTC-related multi-train collisions (typically 2 or 3 trains involved; see example in Figure 1), factors included GPS signal anomalies, incomplete PTC installations, and improper PTC maintenance. Multiple injuries, commonly fatal, often result in any given incident, in addition to as much as $25M in property damage per incident reported. Recognizing this, the NTSB has long advocated for the implementation of PTC, calling on the FRA to incorporate new technologies into the existing PTC system that prevents certain train collisions.[10]

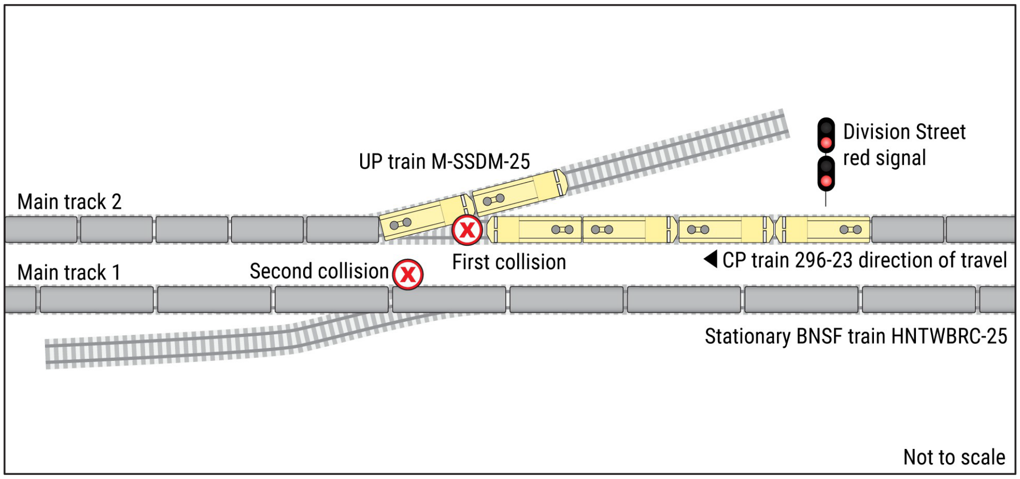


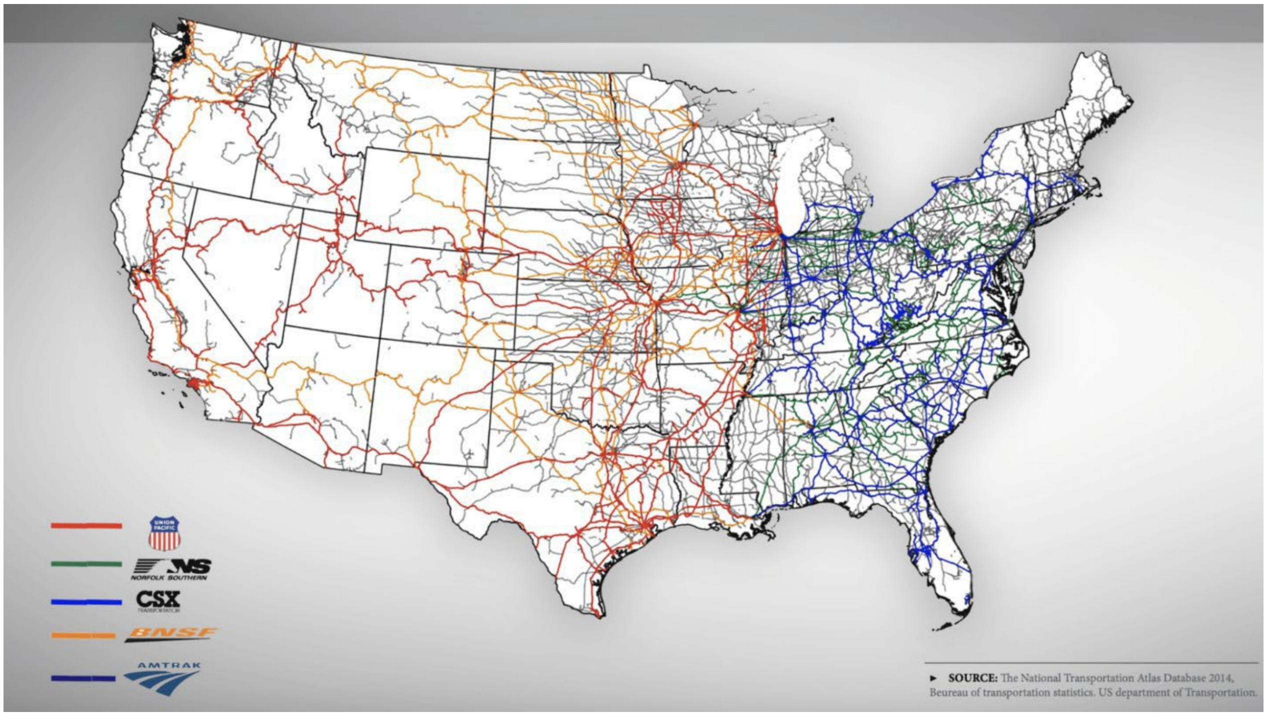
Figure 1: Railway Raking Collision and Impact with Standing Train due to PTC Failure[11]

Both freight rail and intercity passenger rail, including Amtrak, utilize PTC. Railroads must report to the FRA on the number of PTC system failures that occurred in the previous reporting period, and summarize actions taken to reduce the frequency of PTC system failures or malfunctions.[12] However, current regulations do not require the railroads to delineate those PTC failures occurring because of degraded GPS availability and quality.

The Volpe team met with MxV Rail, which provides independent engineering and technology services for freight rail, at their Pueblo, CO facility in August 2023.[13] During this site visit, Volpe ascertained that MxV Rail possesses in-house capability to support the PNT needs of freight rail operators, independent of government resources. Furthermore, EO 13905 applies directly to Federal transportation assets and critical infrastructure, but not to commercial operators. Thus, Volpe and FRA redirected the pilot project to Amtrak as the use case.

Amtrak's operation of its trains brings its own unique PNT challenges. Urban canyons, train stations under covers or underground (see example in Figure 2), and rail tunnels all block GPS signals from reaching on-board receivers. GPS repeaters cannot mitigate this issue, as their use violates spectrum restrictions and GPS protections. Starting a train under a cover hampers initialization of the given train's position, velocity, and time solution, causing delays. Losing GPS signals while en route forces reliance on dead reckoning, the process of calculating the current position of the train based on the knowledge of the last verified position along with acceleration, speed, and angular rate.[14] Complementary PNT sources, described in Section 6, become the sole source of needed data under these conditions.

Figure 2: Amtrak trains at Chicago Union Station[15]



► SOURCE: The National Transportation Atlas Database 2014, Beureau of transportation statistics. US department of Transportation.

Figure 3: U.S. Railroad Lines by Ownership[16]

Furthermore, Amtrak owns only 3% of the 21,400 route-miles traveled by its trains; the rest are mostly owned by freight railroads, as shown in Figure 3.[17] Therefore, the operation of Amtrak trains on rail lines not owned by Amtrak must utilize the host rail operators' PTC implementation, namely I-ETMS (Interoperable Electronic Train Management System). Thus, Amtrak requested that the Pilot Project focus PNT efforts on rail service along these rail networks. Additional discussions revealed GNSS to be Amtrak's primary source of precision timing, underscoring their need for assured, resilient PNT.

As a result, this project seeks to satisfy the U.S. DOT response to EO 13905 for rail, while considering the PNT needs of Amtrak, by identifying suitable equipment for Amtrak PNT resiliency. This equipment must function in GPS-challenged environments while providing interoperability with freight rail networks.

DOT, FRA, and Volpe Actions

In response to EO 13905, the U.S. DOT has undertaken the following broad actions:

- PNT Vulnerability Assessment and Testing
- Pilot Projects – discussed below
- PNT Profile Adoption and Adaptation
    - Application of National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to the PNT ecosystem
    - Provides a flexible framework for users of PNT services to manage risks when forming and using PNT signals and data
- Implementation of National R&D Plan on PNT Resilience
- Protect, Toughen, Augment, Adopt (PTAA)
    - Ensure Performance Monitoring of Space-Based Civil PNT Services
    - Implement Interference Monitoring Capabilities to Identify, Locate, and Attribute PNT Service Interruptions and Threats = IDM
    - Prevention of Harmful Interference
    - Facilitate international coordination for development of monitoring standards
    - Authenticate signals and harden user equipment (receiver/antenna/algorithms)
    - Implement and utilize GPS augmentations and Complementary PNT services
    - Facilitate adoption of Complementary PNT into end-user applications
- Work with Department of Homeland Security (DHS) on PNT Resilience Contract Language
- Complementary PNT technology portfolio
    - 2020 CPNT and GPS Backup Technologies demonstration
    - 2024 CPNT portfolio
    - Volpe Clearinghouse for high-TRL CPNT technologies

OST-R, in partnership with FRA, developed a Pilot Program Plan focused on addressing GPS jamming and spoofing in rail operations. OST-R put an interagency agreement in place with the Volpe National Transportation System Center (Volpe Center) to support this Pilot Program. A primary goal of the U.S. DOT Pilot Program is to apply the NISTIR 8323 Foundational PNT Profile (discussed in Section 0) through an application-based effort.

Volpe Center activities include:

- Stakeholder engagement with FRA and Amtrak;
- Test plan development;
- Research and market survey of anti-jamming and anti-spoofing technology;
- CPNT technology research and preliminary assessment;
- Jamming/spoofing mitigation technology procurement;
- Equipment setup and installation on test platform;
- Testing in an active jamming/spoofing event;
- Processing and analysis of collected data; and
- Final report including
  - Recommendations and plans for a follow-on Pilot Project,
  - Advising FRA on how this pilot project informs future rulemaking, and
  - Working with Amtrak on implementation of solutions on operational trains.

2. NIST Foundational PNT Profile

In addition to development and implementation of a Pilot Program, EO 13905 seeks to protect the national and economic security of the United States from the disruption or manipulation of systems that provide or use PNT data and information vital to the functioning of critical infrastructure and technology-based industries. The EO directs the Department of Commerce to develop PNT profiles that address the four components of responsible use of PNT:

1. Identify systems that use or form PNT data.
2. Identify PNT data sources.
3. Detect disruption and manipulation of the systems that form or use PNT services and data.
4. Manage risk regarding responsible use of these systems.

National Institute of Standards and Technology (NIST) Internal Report 8323 (NISTIR 8323), published in February 2021, applies the NIST Cybersecurity Framework (CSF) to the PNT ecosystem.[18] The NIST Foundational PNT Profile (referred to hereafter as the "PNT Profile") provides a flexible framework for users of PNT services to manage risks when forming and using PNT signals and data.[19] The PNT Profile can be applied to all organizations that use PNT services, regardless of the level of familiarity or knowledge they have with the CSF. All organizations can benefit.

The PNT Profile is voluntary and entirely recommendatory in nature, intended to be a foundational set of guidelines. It does not: represent any enforceable regulations; define mandatory practices; establish compliance standards; or carry any statutory authority. Sector Risk Management Agencies and other entities may wish to augment or further develop their own PNT cybersecurity efforts via full or partial implementation of the PNT Profile recommended practices. Any implementation of its recommendations will not necessarily protect organizations from all PNT disruption or manipulation. Each organization is encouraged to make their risk management decisions in the context of their own cyber ecosystem, architecture, and components. The PNT Profile's strategic focus is to supplement existing resilience measures and elevate the postures of less mature initiatives.

Intended Use

The PNT Profile is a flexible tool that can be used by an organization to help meet mission and business objectives that are dependent upon the use of PNT services. The PNT Profile can help organizations determine risks based on their assessments of the potential impacts of manipulation or the disruption of PNT services to their own business and operational objectives, and to prioritize cybersecurity activities based on those objectives. Additionally, the PNT Profile can be used to guide organizations as they identify areas where standards, practices, and other guidance could help manage risks to systems that use PNT services. An organization can use the PNT Profile in conjunction with its systematic process for identifying, assessing, and managing risk. NIST acknowledges the existing efforts being undertaken by individual entities to address the responsible use of PNT services in their sectors, and the PNT Profile is intended to complement—not replace—those efforts. NIST also encourages the development of sector-specific guidance if more specific risk-management efforts are required.

Cybersecurity Risk Management

Cybersecurity risk management is the ongoing process of identifying, assessing, and responding to risk as related to an organization's mission objectives. To manage risk, organizations should understand the likelihood that a cybersecurity event will occur and consider the potential impacts of that event. An organization should also consider statutory and policy requirements that may influence or inform cybersecurity decisions. The PNT Profile supports and is informed by the cybersecurity risk management process.

Using the PNT Profile, organizations can make more informed decisions—based on business needs and risk assessment—to select and prioritize cybersecurity activities and expenditures that help identify systems dependent on PNT, identify appropriate PNT sources, detect disturbances and manipulation of PNT service, manage the risk to these systems, and ensure resiliency to their user base.

It also provides a starting point from which organizations can tailor their approach to manage risk to their PNT services and data. A customized approach provides the most appropriate measures, processes, and prioritization of resources for the reliable and efficient functioning of critical infrastructure applications. Organizations can use the PNT Profile in conjunction with existing risk management processes. The PNT Profile assumes that the organization implements cybersecurity risk management processes and provides additional risk management considerations specific to PNT.

PNT Profile Framework Description

Created through collaboration between industry and government, the NIST CSF provides prioritized, flexible, risk-based, and voluntary guidance based on existing standards, guidelines, and practices to help organizations better understand, manage, and communicate cybersecurity risks.[20] Although it was designed for organizations that are part of the U.S. critical infrastructure, many other organizations in the private and public sectors (including Federal agencies) may use or implement the NIST CSF. The framework consists of three main components:

1. The **Framework Core** provides a catalog of desired cybersecurity activities and outcomes using common language. The Core guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management process.
2. **Framework Implementation Tiers** provide context for how an organization views cybersecurity risk management. The Tiers help organizations understand whether they have a functioning and

repeatable cybersecurity risk management process and the extent to which cybersecurity risk management is integrated with broader organizational risk management decisions.

3. **Framework Profiles** are customized to the outcomes of the Core to align with an organization's requirements. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization.

The NIST.IR.8323 Foundational PNT Profile describes the five Framework Core functions as follows:

1. Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational to the effective use of the Cybersecurity Framework, enabling an organization to focus and prioritize its efforts in a manner consistent with its risk management strategy and business needs.
2. Protect – Develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services. The activities in the Protect Function support the ability to limit or contain the impact of a potential PNT cybersecurity event.
3. Detect – Develop and implement the appropriate activities to sense and identify the occurrence of a cybersecurity event. The activities in the Detect Function enable the timely discovery of PNT cybersecurity events.
4. Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The activities in the Respond Function support the ability to contain the impact of a potential PNT cybersecurity event.
5. Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The activities in the Recover Function support timely recovery to normal operations to reduce the impact of a PNT cybersecurity event.

When considering the five functions, **Identify** and **Protect** can further be characterized as taking place before a PNT cybersecurity event or attack, **Detect** and **Respond** during a cybersecurity attack, and **Recover** during and/or after a cybersecurity attack (see Figure 4). When considered together, these functions provide a high-level, strategic view of the life cycle of an organization's management of PNT cybersecurity risk.

Applying the NIST profile to the PNT Pilot Project for rail yields the following outline for project activities. Initially, the pilot project will identify Amtrak's PNT (GNSS, CPNT) equipment and needs; identify proposed protection and detection upgrades; and bring PNT equipment to U.S. Government GPS-jamming and -spoofing events for initial assessment of rail's ability to respond to a GNSS attack. In later phases, the pilot project will address the remainder of the profile functions as follows:

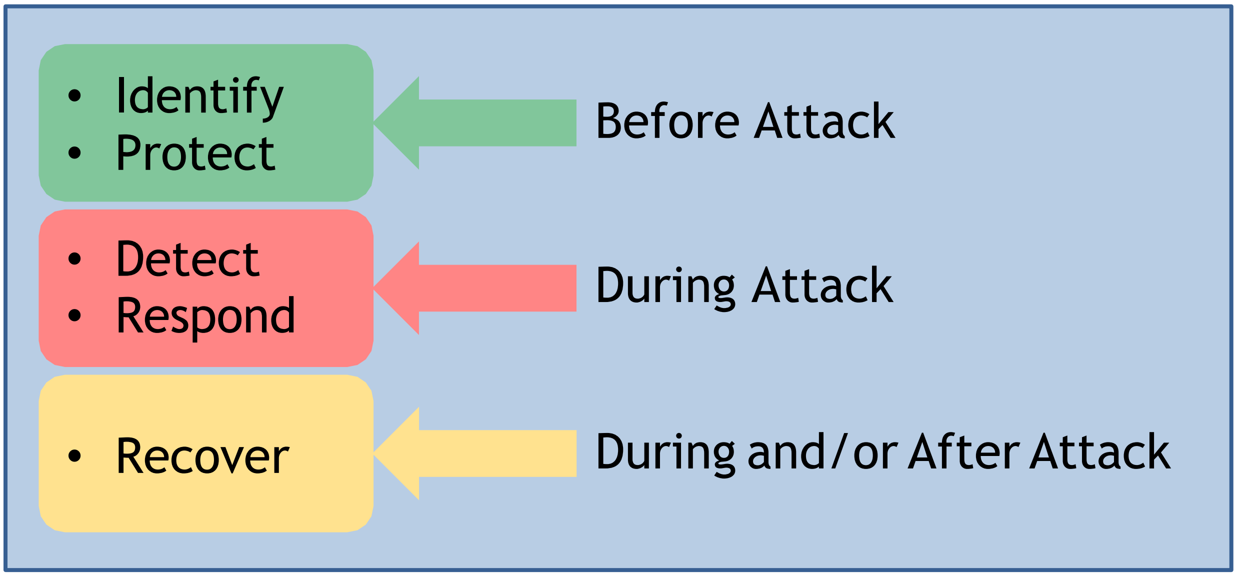


Figure 4. Five Functions within the NIST PNT Profile

- Operational test of PNT equipment to validate rail's ability to <u>respond</u> to GNSS attack;
- Utilize a rail testbed to validate rail's ability to <u>respond</u> to GNSS attack;
- Evaluate more advanced elements for <u>protection</u> and <u>detection</u> (e.g. navigation warfare antennas, anti-jam devices);
- <u>Detect</u> benign GNSS interference sources;
- Formulate plans to <u>respond</u> to and <u>recover</u> from GNSS events; and
- Inform FRA planning for the future of PTC.

3. PNT Pilot Program Approach

Rail PNT – Phase I

As discussed in the preceding sections, modal compliance with EO 13905 incurs mode-specific approaches. For FRA and rail, compliance with the Executive Order translates to a PTC focus. Subsequently, consideration of Amtrak passenger rail service as the use case for FRA's PNT resiliency entails unique challenges requiring unique solutions.

Utilizing the Volpe Center's PNT experience with the Maritime Administration, the approach for FRA and Amtrak began with understanding Amtrak's PNT equipment and needs.[21] Several discussions with FRA and Amtrak revealed that outside of the Northeast Corridor (NEC), Amtrak PNT sources include the Wabtec NSM-04 GPS receiver paired with an included Sinclair multi-use antenna, and wheel tachometry. The NSM-04 pictured in Figure 5 is a GPS-only receiver lacking the ability to receive signals from other GNSS constellations such as Europe's Galileo system.[22] In addition to GPS signal reception, the Sinclair unit also provides Wi-Fi and 4G cellular connectivity for data links between trains and operation centers.[23] Note that these are not considered signals-of-opportunity CPNT sources in this application. Wheel tachometry provides limited dead reckoning ability, considered usable for a maximum of 10 miles traveled after the start of continuous GNSS disruption.

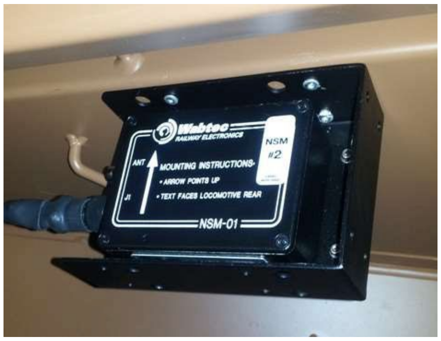


Figure 5: Wabtec NSM-04 GPS receiver unit

The NSM-model receiver and Sinclair antenna each lack jamming and spoofing protection and detection capability. Identification of suitable candidates for equipment replacement thus leads the PNT Profile development. Candidate receivers and antennas are discussed later in this report.

The Volpe team brought the identified candidate equipment to a U.S. Government GPS jamming and spoofing event, described in detail in Section 4. This event provided large-scale scenarios approximating real-life events, to gauge receiver and antenna performance in an active jamming and spoofing environment. These tests resulted in an initial assessment of the ability of rail to respond to GNSS attacks.

The Pilot Project also produced a preliminary assessment of complementary PNT (CPNT) sources of interest in response to Amtrak's dead reckoning needs. The vulnerabilities of and dependence on PNT services from GPS have increased significantly for the public sector. Reducing economic and safety risk exposure due to dependence on GPS leads to considerable investment in CPNT services. Freight Rail operators and Amtrak have identified three candidates of interest: Ground Penetrating Radar, Machine Vision, and Ultra Wide Band (UWB). Details for these CPNT sources are provided in Section 6.

Lastly, the Pilot Project included preliminary planning for a Radio Frequency (RF) survey. This survey will characterize environmental and RF factors that impact the performance of on-board PNT sources. Benign RF interference sources include both on-board equipment in operation and the surrounding environment through which operations occur.

The culmination of the FRA PNT Pilot Project is this report which includes test data analysis, rail PNT recommendations, and plans for a second phase of this effort.

Maritime PNT – Phase 1 and 2

In alignment with the objectives of the overall PNT Pilot Program, the maritime environment was initially identified as having important critical infrastructure suitable for the testing of PNT resiliency requirements.[24] The first phase focused on MARAD's Ready Reserve Force (RRF) vessels and provided findings and recommendations that:

1. Identified specific shipboard systems aboard RRF vessels that rely on or generate PNT data.
2. Identified a complementary PNT data source suitable for the maritime operating environment to diversify acquisition of PNT data from a non-GPS source—through operational testing and data collection.
3. Detected the disruption and manipulation of PNT services in actual and simulated marine environments—through successful testing of shipboard PNT equipment in both laboratory and real-world operational settings, under normal and disrupted/manipulated conditions.
4. Provided MARAD with a framework to manage the associated risks to the shipboard systems, networks, and assets dependent on PNT services—by identifying equipment that provides protection (i.e., shields and/or defeats manipulation) and augmentation (i.e., utilizes complementary PNT signals), and sharing that information with key stakeholders.

In a second phase, executed concurrently with rail PNT work, the Volpe Center (in coordination with the MARAD Office of Safety, conducted at-sea testing of the controlled reception pattern antennas identified in the first phase. The goal of these sea trials was to evaluate how well the protective technologies perform during periods of intentional manipulation and unintentional interference or outages to GPS in an actual operating environment. Volpe Center activities include:

- Stakeholder engagement with vessel owners and operators

- Test plan development
- Research and market survey of non-CRPA anti-jamming and anti-spoofing technology
- CPNT technology research/pre-assessment
- CRPA and other jamming/spoofing mitigating technology procurement
- Lab-based dry runs of simplified scenarios that validate and debug the test approach
- Equipment setup and installation on test vessels(s)
- Sea trials with installed technology-under-test, truth systems, and supporting data collection
- Processing and analysis of collected data
- Submission of a final report, and
- Work with MARAD on implementation of solutions on RRF vessels.

The initial phase of the MARAD PNT pilot project provided the outline for the Rail PNT effort. The latter followed a similar approach of stakeholder engagement, GNSS technology test and evaluation, CPNT assessment, and test data analysis informing conclusions for the application of the PNT Profile to passenger rail.

Overview of DOT CPNT Evaluation

In support of the U.S. DOT Complementary Positioning, Navigation and Timing (CPNT) Technologies, Rapid Phase 1 effort, the U.S. DOT Volpe Center awarded contracts to nine CPNT technology vendors In June 2024. These awards enable U.S. DOT to conduct real-world field tests of commercial PNT technologies to facilitate adoption into systems that depend on secure and reliable PNT services. To this end, DOT has developed scenarios to represent critical infrastructure use-cases for positioning, navigation and timing functions which will be used to evaluate the performance of the CPNT technologies. Testing will revolve around a series of preplanned scenarios designed to exercise the positioning and/or timing capabilities of each CPNT technology. Scenarios will be executed for static timing (time transfer and time synchronization), dynamic timing, indoor and outdoor static positioning, and outdoor dynamic positioning for vehicle-based, dismounted, and airborne use-cases. All scenarios will be run in nominal conditions, which will determine baseline performance. Select timing and positioning scenarios will be run in adverse conditions, which will be used for evaluating operational resiliency. Participation in each scenario type will be dependent on CPNT use-cases and capabilities.

4. Equipment Testing

Working with FRA and Amtrak, Volpe identified PNT risks in rail operations across the U.S. Phase I of this effort included equipment live testing in a DOD-managed active jamming and spoofing event, to determine the capabilities of the existing and proposed PNT equipment in GPS compromised/denied environments. Subsequent analyses by Volpe informed recommendations for PNT resiliency and definition of an in-situ test plan in partnership with Amtrak.

NAVFEST 2024 provided an opportunity for controlled active GPS-denial testing on devices being explored in support of EO 13905. Testing took place at the White Sands Missile Range (WSMR) located in Socorro County, NM, near the towns of Carrizozo and San Antonio. WSMR is a national asset, critical for enabling national security modernization through independent development testing, operational testing, and evaluation. White Sands Missile Range provides unmatched infrastructure and capabilities to test, evaluate, and train emerging technologies in a multi-domain operations environment. Comprised of a 3,200 square mile area that is roughly the size of Rhode Island and Delaware combined, White Sands Missile Range supports the Army, Navy and Air Force, as well as commercial and international users on a reimbursable basis while conducting more than 3,000 tests annually. [25]

Further details of DOT participation in this test event are provided by the U.S. DOT Volpe Center in the test plan document, "NAVFEST 2024 | DOT PNT Test Plan (CUI) – March 2024." Test and facility details are Controlled Unclassified Information (CUI) provided by the USAF AFMC 746th Test Squadron, the host organization for NAVFEST.

Equipment under Test

The following receiver/antenna pairs (tabulated in Table 4) were tested to evaluate PNT performance under a diverse array of GPS-challenged and GPS-denied environments.

Freight rail operators have turned to the Wabtec GoLinc Precision Navigation Module (PNM), pictured in Figure 6, for their PTC and PNT on-board receiver equipment. [26] Wabtec is a major provider of locomotive-based equipment providing PNT and communications for I-ETMS integration, with GoLinc PNMs installed on trains operated by CSX Transportation, Norfolk Southern Railway, Union Pacific Railroad, BNSF Railway, and other major freight rail providers. The PNMs incorporate multi-GNSS capability through their embedded Septentrio AsteRx-SB33 Pro GNSS receivers, which contain anti-jamming, anti-spoofing, and interference mitigation and monitoring technology. [27] Given the multi-GNSS capability, anti-jamming and -spoofing technology, and widespread adoption in the rail industry (including I-ETMS integration), the GoLinc PNM became the sole choice for initial receiver evaluation for Amtrak's purposes.

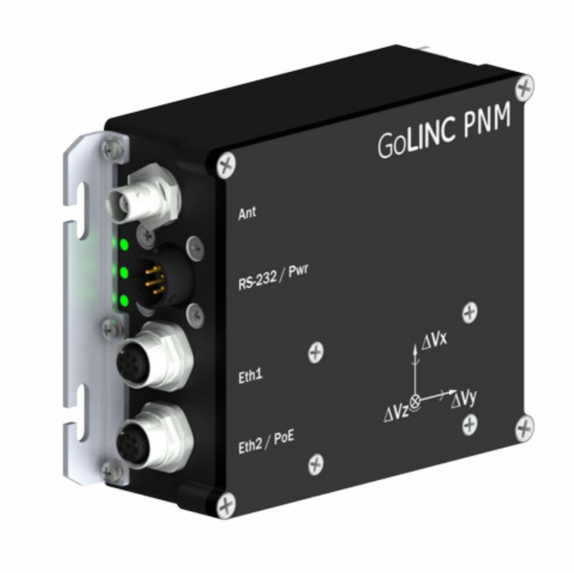


Figure 6: Wabtec GoLinc PNM unit

A few candidate antennas suitable for pairing with a Wabtec GoLinc PNM were selected based on MARAD experience, market research, and discussions with FRA and Amtrak. A further consideration for antenna selection is installed antenna height, limited to approximately 4 inches for tunnel roof clearance and margin (see Figure 7).[28] This excluded a number of promising candidates, such as the Tallysman AJ977XF anti-jam antenna, which is 7 inches in height in its optimum installation.

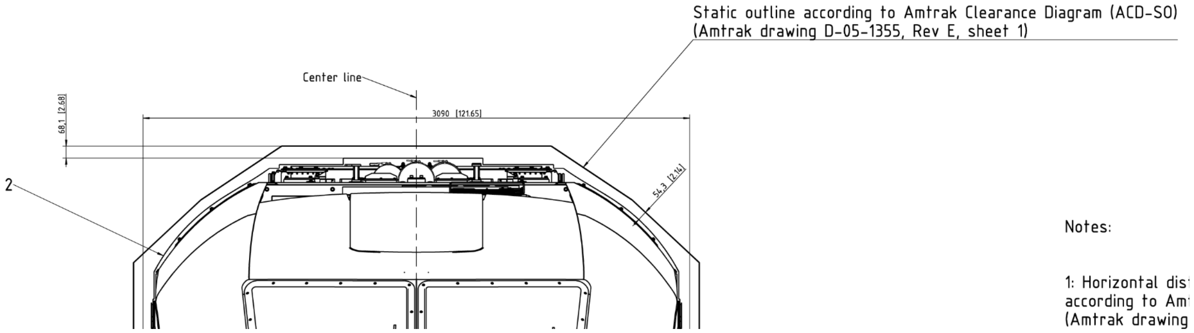

Static outline according to Amtrak Clearance Diagram (ACD-SO)
(Amtrak drawing D-05-1355, Rev E, sheet 1)
Center line
3090 [121.65]
68,1 [2.68]
54,3 [2.14]
2
Notes:
1: Horizontal dis
according to Am
(Amtrak drawing

Figure 7: Amtrak schematic of train height with maximum antenna clearance indicated

Current Sinclair antennas in Amtrak service rely on 4G networks which cellular providers are replacing with 5G service. Thus Sinclair is currently developing a prototype 5G/LTE-capable replacement, the SM714 pictured in Figure 8. It features an IP67 rating, built-in tri-band multi-constellation GNSS (GPS, Galileo, GLONASS, BeiDou) module, and wideband cell ports covering all major 5G/LTE bands.

The aforementioned freight rail operators typically pair each of their PNMs with the Tallysman TW3972 unprotected antenna.[29] This is a multi-band GNSS antenna capable of receiving GPS/QZSS-L1/L2/L5, GLONASS-G1/G2/G3, Galileo-E1/E5a/E5b, BeiDou-B1/B2/B2a, and NavIC-L5 bands in addition toregional SBAS signals. The Tallsyman unit is also ruggedized for exterior installations. Volpe selected the

TW3972XF variant for its ability to filter nearband RF interference, to further determine the impact of this capability versus the unfiltered Sinclair unit, and for greater parity with protected solutions.

Figure 8: Sinclair SM714 Antenna prototype

Figure 9: Tallysman TW3972XF GNSS Antenna

Through market research and MARAD experience, the Volpe team selected the NovAtel Hexagon GAJT-410ML as the candidate protective (anti-jam, anti-spoof) solution for rail.[30] The Hexagon antenna shown in Figure 10 is an L1 and L2, four-element controlled reception pattern antenna (CRPA) array with nulling capability. The nulling algorithm belongs to a class of adaptive beamforming techniques where the complex array weighting vector is found as a solution to a constrained optimization problem. The algorithm solves for the constrained weighting vector by minimizing the error between the constrained solution and quiescent solution subject to a minimum power constraint. In the presence of a jammer or a strong spoofer, the constrained weighting vector solution effectively results in a good approximation of the quiescent pattern with a null placed in the direction of the jammer or spoofer. This is considered an adaptive beamforming technique because a priori knowledge of the direction of the jammer or spoofer is not needed, and its beamforming pattern adapts in real-time to a dynamic jamming or spoofing environment. Note that the GAJT falls under International Traffic in Arms Regulations (ITAR) export controls, due to its number of elements and null depth.[31]

Figure 10: Hexagon GAJT-410ML Antenna

Figure 11: GPS Source MRPA Antenna

With Amtrak service running and/or connecting to Canada and Mexico, equipment installed onboard must comply with ITAR restrictions, necessitating selection of a candidate ITAR-clear protective solution. (Note that these restrictions are due to be lifted by the end of 2025.) GPS Source, a subsidiary of General Dynamics Mission Systems, introduced its Modified Reception Pattern Array (MRPA) Antenna, depicted in Figure 11. The MRPA is a single-element, active horizon-nulling GNSS antenna supporting the GPS (L1, L2, L5), GLONASS (L1, L2, L3), and GALILEO (E1, E5, E6) bands.[32] It provides protection by nulling terrestrial interferences arriving at low elevation angles (minimum 20 dB of rejection at 10°-20° elevation angles). Its radome protects against UV, rain, lightning, chemical, and jet fuels, and has passed qualification testing for salt-spray, humidity, and shock and vibration. The MRPA design characteristics mean complete ITAR-compliance, hence MRPA's availability to defense, civil, and commercial customers.

Within the scope of this effort, no additional receivers, antennas, or other anti-jam/anti-spoof devices were evaluated. Additional candidates for future consideration are discussed in Section 8.

Test Scenarios and Schedule

NAVFEST 2024 provided a nightly schedule of scenarios over the span of two weeks with adverse conditions of jamming and spoofing. Variations in waveform types, power levels, location of jammers and threat types defined the different scenarios.

Table 1 describes the high-level types of scenarios. More detailed information is provided in subsequent test matrices.

Table 1. Scenario types and descriptions

Acronym	Short Name	Description
Spoofing Scenarios		
ET	Emerging Threat	GPS defense that provides emerging threat jamming from a single location
CET	Complex Emerging Threat	GPS defense that provides complex emerging threat jamming from a single location
Jamming Scenarios (CT – Conventional Threat)		
AL	Area Low Power	GPS jamming defense that provides jamming from one small location radiating 360 degrees
AM	Area Medium Power	GPS jamming defense that provides medium power jamming across a large area
AH	Area High Power	GPS jamming defense that provides high power jamming across a large area
LH	Line High Power	GPS jamming defense that provides a nominal line of jamming
NH	NOP High Power	GPS jamming defense that provides jamming from a high elevation location
CH	Corridor High Power	GPS jamming defense that provides jamming along one stretch of road (RR7)
BMA/BMB	Blink (Pattern A / Pattern B)	Jammers will vary in number of jammers in sequence & notional ON/OFF schedule for a period of 1 hour
RO	Rotate	Jammers will rotate as single emitters from 1-8 in a sequence
CUSTOMER	Customer	Custom jamming pattern utilizing customer technology

USAF Jamming equipment comprised the following:

- CT Jammers
  - Outer Ring: 8 x HPJs (1000W each) – HX01-HX08
    - 7 x 30x30 Micronetixx Antennas
    - 1 x 60x60 Micronetixx Antenna
  - Inner Ring: 8 HPJs (300W each) – NX01-NX08; 30x30 Helix Antennas
- CET/ET Jammer: 1 x PBJ – EX01A, EX01B; 30x30 Micronetixx Antennas
- Cover Jammers: 7 x HPJs – CX01-CX07; 60x60 Micronetixx Antennas
- Airborne Jammer: 1 x PJB – ABJ-II
  - 80x80 Omni Antenna L1
  - 60x60 Omni Antenna L2

The nightly test matrices for NAVFEST 2024 are given in Table 2 and Table 3. At the start of each night, a Knock-Off (KO) jamming event was scheduled before each of the ET and CET scenarios. This is meant to "knock-off" GPS receivers from their valid solution. The table cells are color coded to indicate high-level threat type: ET – yellow, CET – orange, CT – green). The second line within each cell indicates the USDOT test team’s site location, and motion type for each scenario. NA designates scenarios that were cancelled by the NAVFEST operators. The local time represents 15-minute periods ending at the displayed time. Scenario start- and end-times are approximate. In addition to ground-based jammers, an airborne jammer (ABJ) was active for some scenarios.

Table 2. Test Matrix - Week 1

Date	7-May-24	8-May-24	9-May-24	10-May-24
Night ID	1	2	3	4
0:15				
0:30				
0:45	KO (10 Min) Melton | Static	NA	KO (10 Min) Melton | Static	KO (10 Min) Stallion | Static
1:00	ET Melton | Static	NA	ET Melton | Dynamic 1	ET Stallion | Static
1:15				
1:30				
1:45	KO (10 Min) Melton | Static	KO (10 Min) Melton | Static	KO (10 Min) Melton | Static	KO (10 Min) Stallion | Static
2:00	CET Melton | Dynamic 1	CET Melton | Dynamic 1	CET Melton | Static	CET Stallion | Static
2:15				
2:30				
2:45	AL Melton | Static	AH Melton | Static	AH Melton | Static	AH Convoy | SRC to Phets
3:00				
3:15				
3:30	AL Melton | Static	LH + ABJ Melton | Static	LH + ABJ Melton | Static	AH Melton | Dynamic 1
3:45				
4:00				
4:15	AM Melton | Static	CH + ABJ Melton | Static	CH + ABJ Melton | Static	AH Melton | Static
4:30				
4:45				
5:00	AM Melton | Static	NH + ABJ Melton | Static	NH + ABJ Extended Convoy | SE of Phets to SRC	AH Melton | Static
5:15				
5:30				

Table 3. Test Matrix - Week 2

Date	14-May-24	15-May-24	16-May-24	17-May-24
Night ID	5	6	7	8
0:15				
0:30				
0:45	KO (10 Min) Weap | Static	KO (10 Min) Convoy | SRC to Phets	KO (10 Min) Weap | Dynamic 2	KO (10 Min) Norma Access | Static
1:00	ET Weap | Static	ET Convoy | SRC to Phets	ET Weap | Dynamic 2	ET Norma Access | Static
1:15				
1:30				
1:45	KO (10 Min) Weap | Static	KO (10 Min) Convoy | Phets to SRC	KO (10 Min) Weap | Dynamic 2	KO (10 Min) Norma Access | Static
2:00	CET Weap | Static	CET Convoy | Phets to SRC	CET Weap | Dynamic 2	CET Norma Access | Static
2:15				
2:30				
2:45	BMA Weap | Static	AH + ABJ Convoy | SRC to Phets	BMB Melton | Dynamic 2	AH + ABJ Weap | Dynamic 2
3:00				
3:15				
3:30		LH + ABJ Convoy | Phets to SRC		LH + ABJ Weap | Static + Dynamic 2
3:45				
4:00	RO Weap | Static		NA	
4:15		CH + ABJ Convoy | SRC to Phets		CH + ABJ Weap | Static + Dynamic 2
4:30				
4:45				
5:00	CUSTOMER Weap | Static	NH + ABJ Convoy | Phets to SRC	NA	NH + ABJ Weap | Dynamic 2
5:15				
5:30				

Test Setup

The DOT team conducted operations out of the Mercedes Sprinter van shown in Figure 12 for both static and dynamic operations. The van served as the platform for the ground truth reference system, as well as all devices-under-test. In addition, a WAAS G-III reference receiver was included to aid in identifying periods with interference (i.e. from jamming emitters).

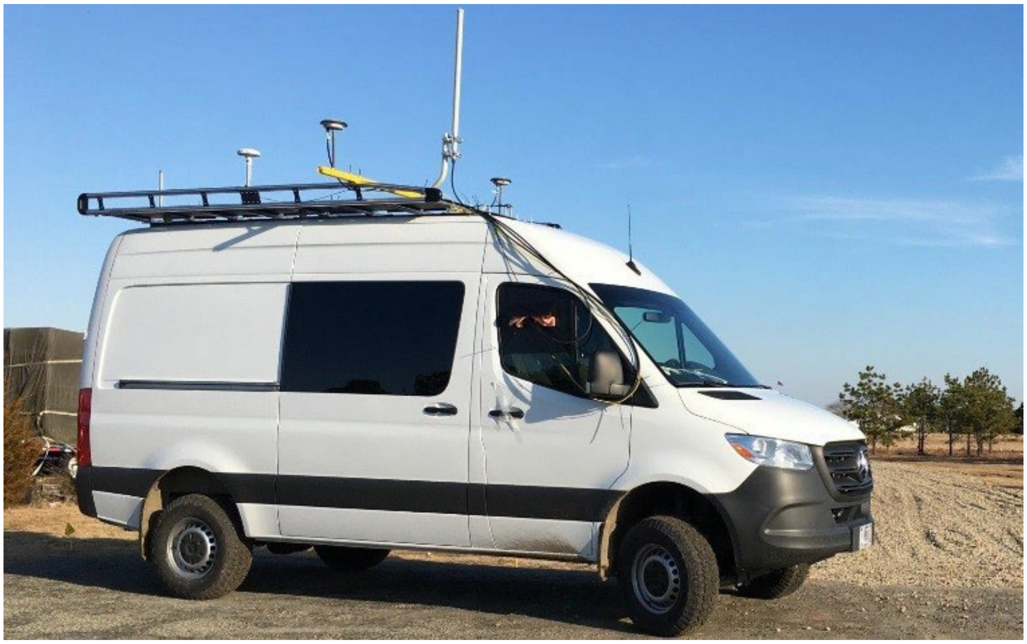


Figure 12: DOT Test Platform

A dual-antenna NovAtel PwrPak7D-E2 (PwrPak7) was used as the ground truth reference system. This PwrPak7 comes integrated with an Epson G370N IMU and was paired with two Tallysman AJ977XF antennas. The PwrPak7 was configured to receive and process signals from multiple GNSS constellations including GPS, Galileo, GLONASS, BeiDou, and SBAS. Additionally, the TerraStar-C PRO Precise Point Positioning (PPP) service was used to enhance the precision of the positioning solution.

Table 4 describes the devices-under-test and their capabilities. One configuration was used for week one, to compare an unprotected technology to a protected technology. A different configuration was used for week two, again comparing an unprotected technology to a protected technology. The same two Wabtec GoLinc PNM receivers were used for both configurations, while the antennas were changed.

Table 4: Equipment as Tested at NAVFEST

Receiver	Antenna	Device/Capability-Under-Test
Wabtec GoLINC PNM 1 of 2	Sinclair SM714 (SNC) *Week 1*	Combination of GoLINC PNM + unprotected tri-band antenna (4G/Wi-Fi/GNSS*) (Representative Amtrak configuration)
	Tallysman TW3972XF (TAL) *Week 2*	Combination of GoLINC PNM + unprotected GNSS patch antenna (Representative freight rail configuration)
Wabtec GoLINC PNM 2 of 2	Gen Dyn MRPA (MRP) *Week 1*	Combination of GoLINC PNM + Horizon-limiting MRPA
	NovAtel GAJT-4 (GJ4) *Week 2*	Combination of GoLINC PNM + 4-element CRPA

* Only GNSS was used. 4G and Wi-Fi were not active, as they are not typically used for rail PNT use-cases. They are used for data communication between Amtrak's servers and trains.

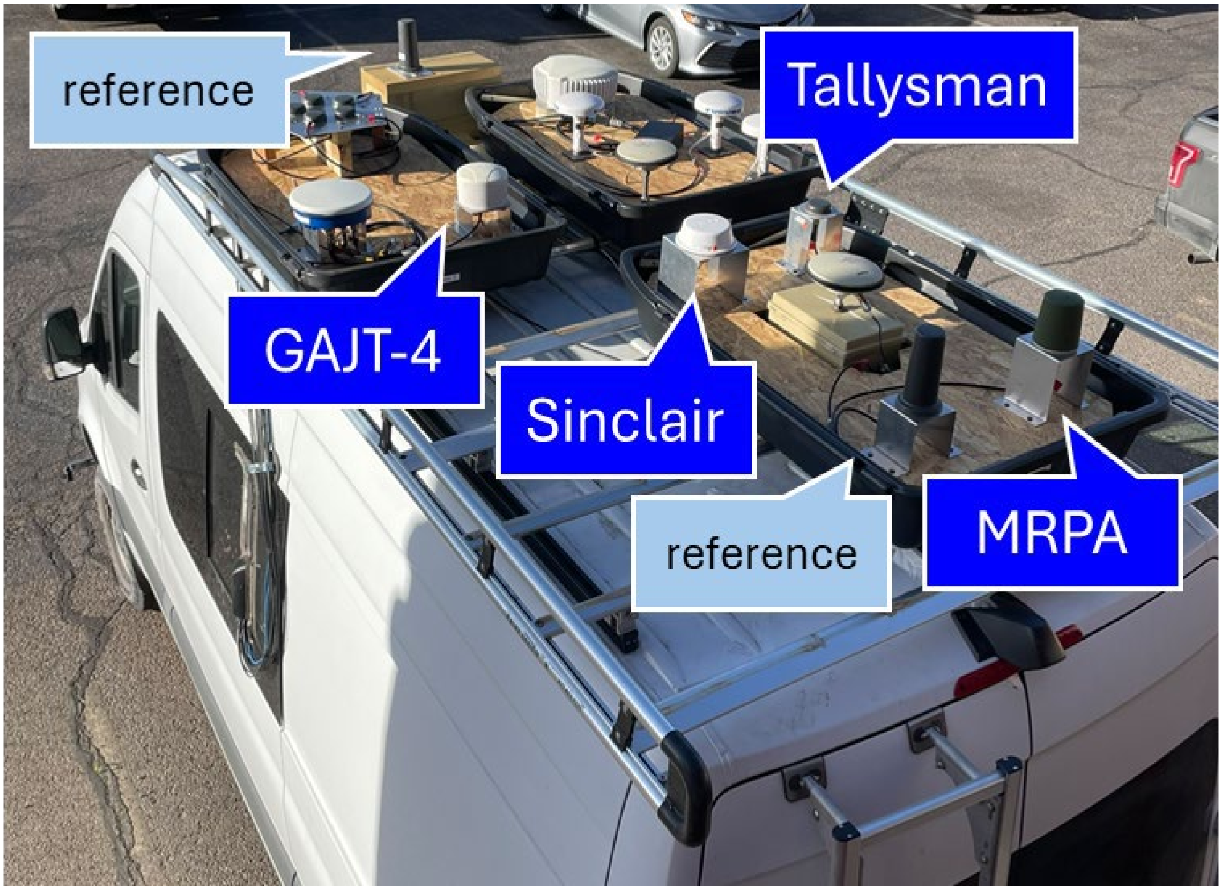


Figure 13: Antenna Installations on DOD Platform

The DOT PNT Team installed the test system antennas on the van's roof rack, as shown in Figure 13.[2] Lateral and/or vertical offsets between the reference antennas, test antennas and pre-surveyed reference points were measured prior to, during, and after testing, as appropriate.

Data Collection

NAVFEST testing occurred during eight nights across two weeks in May 2024. Nights 1–4 spanned May 7 through May 10, and nights 5–8 spanned May 14 through May 17. Reference data was also collected on May 6 (day 0) during clear conditions to serve as ground truth for positioning. Figure 14 shows the locations of all emitters (red) and USDOT site locations (yellow) used during NAVFEST testing.

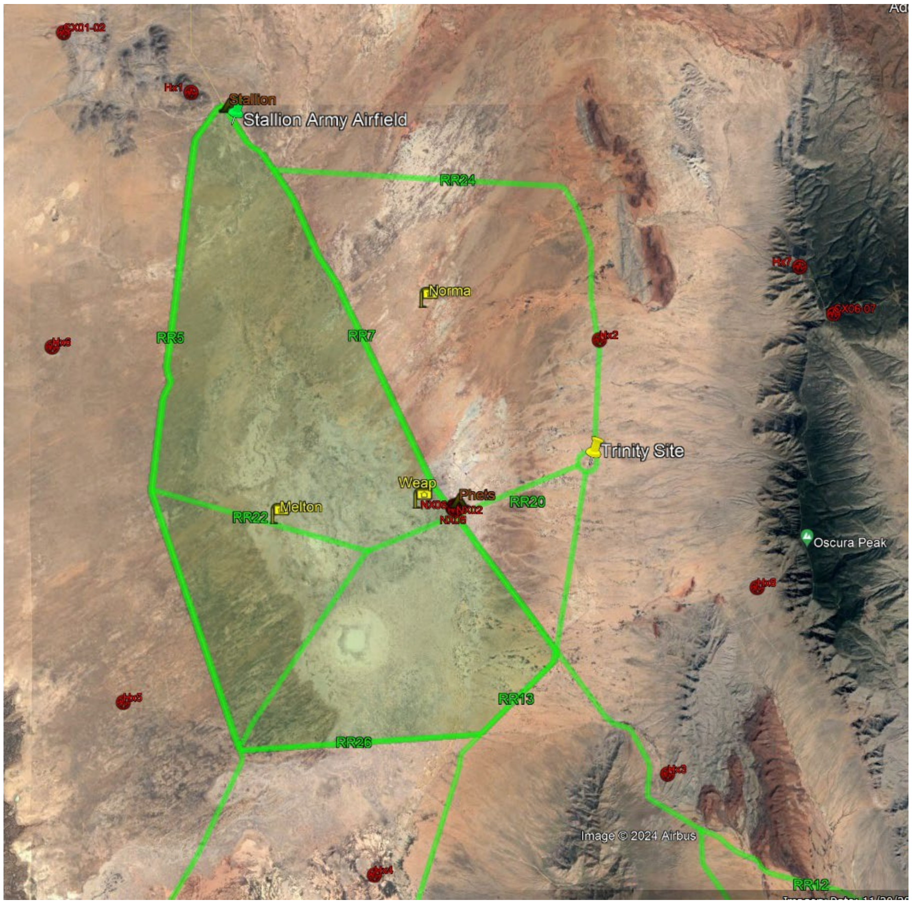


Figure 14. USDOT Site Locations and Emitters at WSMR

Data was collected in the USDOT Sprinter test vehicle during static and dynamic operations at four sites: Melton, Weap, Norma, and Stallion. Benefitting from the dynamic elements inherent in the NAVFEST

[2] The reference antennas were located on the roof proper: one inside the rear case along with other antennas, and the other on a dedicated wood box at the front. The two were centered on the van to form a line along the direction of motion. Vertical alignment with surveyed reference points was handled using a pair of laser levels affixed to metal struts extending from below the front and rear bumpers.

Test Matrix, most data collection took place at pre-surveyed static positions. Where necessary, the test vehicle was aligned with the surveyed points for static data collection using laser levels (affixed to metal struts extending from below the front and rear bumpers). Any remaining horizontal offsets were measured. The conventional threat (CT) scenarios primarily entail static data collection.

To exercise dynamic variables inherent in the transit modes being evaluated, and to fully assess the nulling performance of CRPA technology, the DOT PNT Team executed dynamic data collection. A "Dynamic 1" route involved driving back and forth between two reference points, with brief periods holding the van stationary at each point. Only one Dynamic 1 route was used for testing. A "Dynamic 2" route involved driving with continuous motion. The van also collected data on dynamic routes as part of the convoy that drove along Range Road (RR) 7 between Stallion Range Complex (SRC) at the north end of WSMR and Phets located at the intersection of RR7 and RR20.

5. Data Analysis

This section contains the analysis of the data collected at NAVFEST. Several investigations were conducted to evaluate performance of the devices-under-test with a variety of criteria and conditions. The test scenarios at NAVFEST provided opportunities to evaluate the performance of the devices under a variety of conditions of jamming and spoofing. The investigations are summarized, and key findings are discussed.

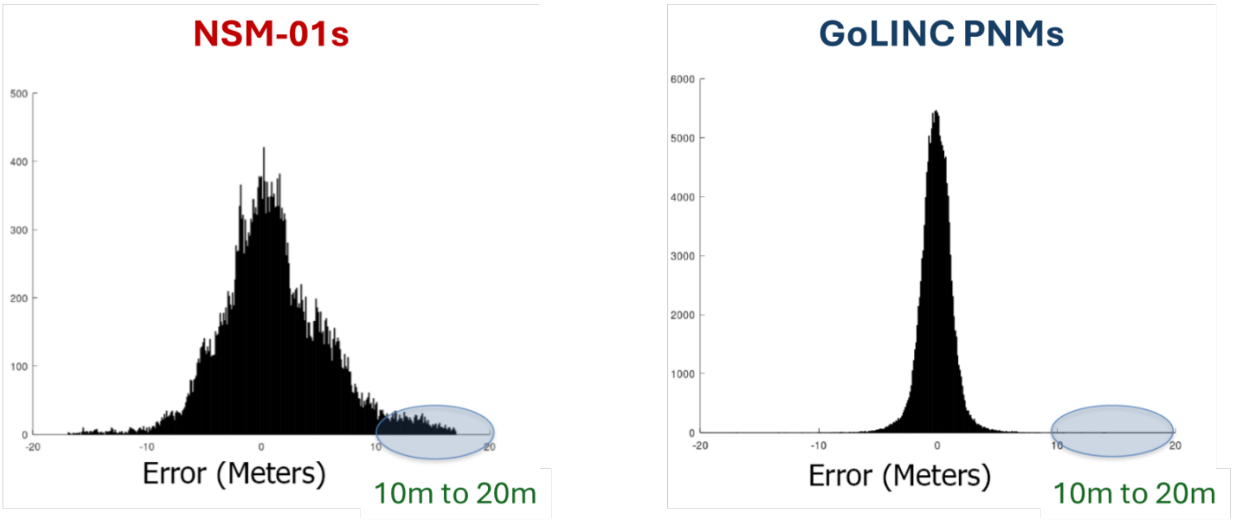


Figure 15: Wabtec-provided position error results for GNSS-challenged environments

Testing prior to the execution of this project suggested that the Wabtec GoLinc PNM exhibits lower horizontal position errors overall with a tighter spread compared to the alternative receiver, as seen in Figure 15. Naval Information Warfare Center (NIWC) testing of the GoLinc PNM receiver for the Alaska Railroad Corporation determined an approximately 25% reduction in error.[33] (Note that the reported data analysis discusses only those improvements obtained with a multi-GNSS receiver vice a GPS-only receiver.) Volpe testing qualitatively supports NIWC's findings.

Detecting Interference

The L1 AGC pulse width data collected by the WAAS G-III reference receiver was used to identify time periods with observed interference. The data was collected during time periods with interference as well as periods without interference for comparison. The full data set was inspected to determine typical baseline values without interference. Thresholds were selected to separate baseline values from values that indicate interference.

Baseline distributions varied by night due to changes in data collection configurations. Figure 16 shows the L1 AGC pulse width histograms grouped by nights with similar configurations.

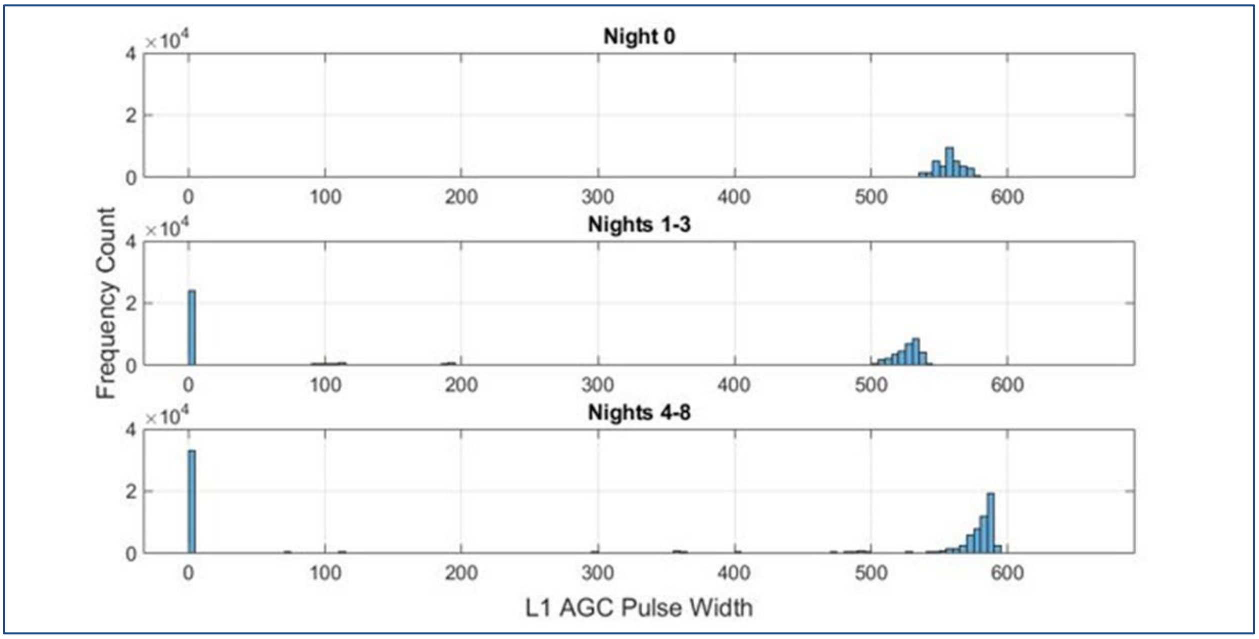


Figure 16. L1 AGC Pulse Width Distribution

The scheduled periods of interference were cross referenced with observed periods of interference. In the case of discrepancies, the observed interference times were used to indicate the scenario start and end times for jamming events. Figure 17 shows a comparison of the scheduled and observed scenario time frames for Night 1 as an example. The ABJ was not scheduled at any time during this night. The full set of time frame comparisons for all nights can be found in Appendix B: NAVFEST Scenario Time Frames.

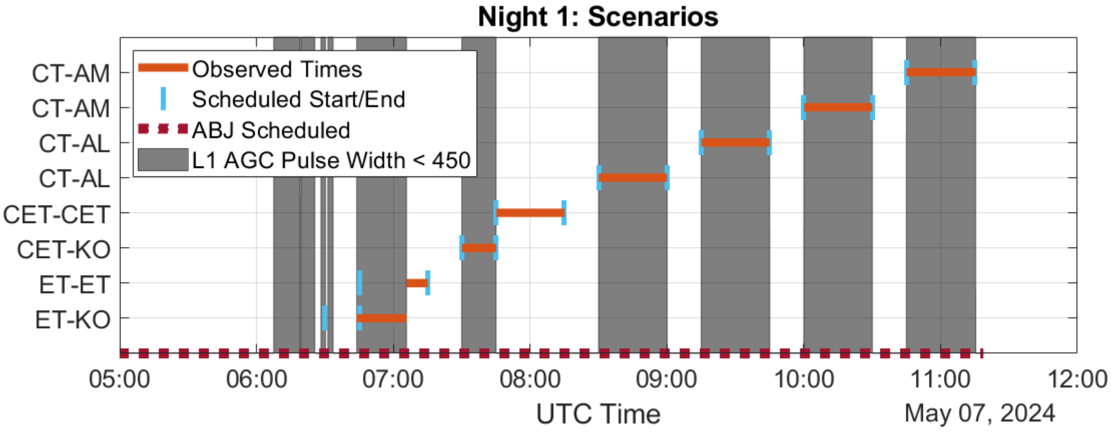


Figure 17. Scenario time frames for Night 1

Signal Availability

The signal availability analysis investigated how often valid horizontal position data (i.e., latitude and longitude) was reported for each device throughout each scenario. The analysis also investigated how many satellites were tracked.

Figure 18 shows how often horizontal position data was reported for each device (vertical axis) throughout each scenario (horizontal axis) throughout NAVFEST. Scenarios are ordered based on scenario type, to visually group similar types of events. Higher values (dark blue) indicate more favorable performance. Each scenario compared a protected device against an unprotected device (MRP vs SNC, GJ4 vs TAL).

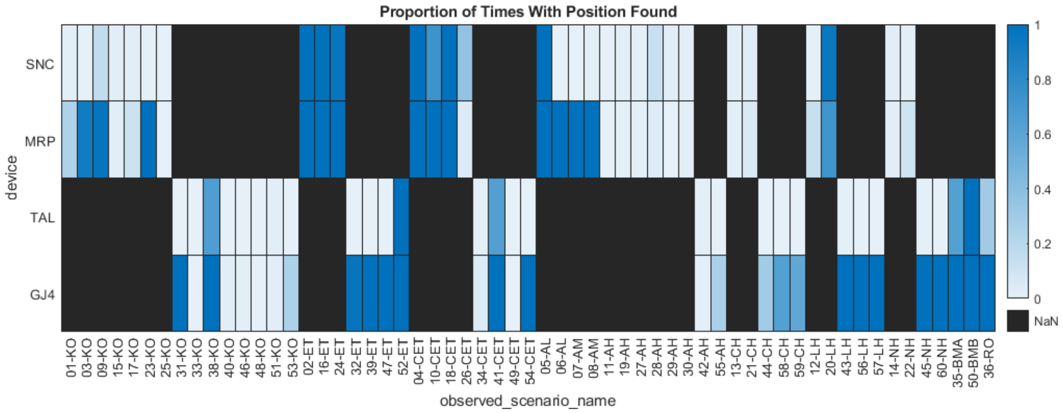


Figure 18. Heatmap with proportion of times a valid horizontal position is reported

Figure 19 shows the mean number of satellites tracked for each device throughout each scenario. Higher values (dark blue) indicate more favorable performance. Devices reported tracked satellite counts at all times throughout the scenarios, with no data drops or missing values.

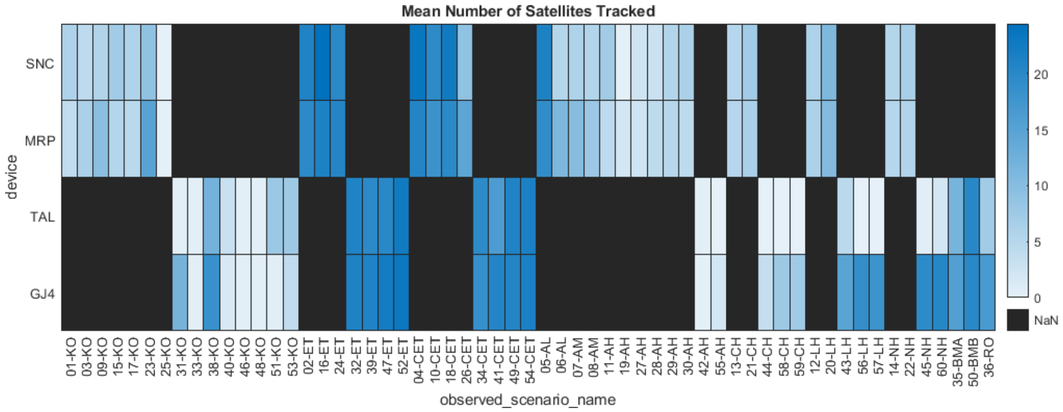


Figure 19. Heatmap with mean number of satellites tracked

The results of the signal availability analysis indicate an overall relative order of performance favoring the protected technologies (MRP, GJ4) over the unprotected technologies (SNC, TAL). However, there are occasional exceptions for certain scenarios.

Static Reference Data

Five reference locations were used for static data collection:

- A: Melton Point 1
- B: Melton Point 2
- C: Weap Point 1
- N: Norma Point 1
- S: Stallion Point 1

Reference position data was collected at each static location under clear conditions during reference time frames to characterize baseline performance for the devices. Horizontal position errors were derived for each device by comparing the reported position to the reference position provided by the PwrPak7 after adjusting for the device's measured physical offset on the van's roof. For certain sites, the van's position and orientation during the reference data collection was marked on the ground. When revisiting the site later, the van could be returned to approximately the same position and orientation by aligning van mounted laser levels with the ground markings. Horizontal alignment was consistently achieved within centimeters. Note that location B was used for reference data collection as well as a hold position in the Dynamic 1 route at Melton. None of the scenarios had fully static data collection at location B.

The following analysis examines the performance of a Wabtec GoLinc PNM receiver compared to an alternative receiver. The MRPA device was split between two receivers during testing. One receiver was the Wabtec GoLinc PNM under test. The other receiver was not a GoLinc PNM, and was used for purposes outside the scope of this report. The baseline horizontal position errors collected during the reference periods for the MRPA were compared directly between the two receivers. Figure 20 shows the distributions of baseline horizontal position errors.

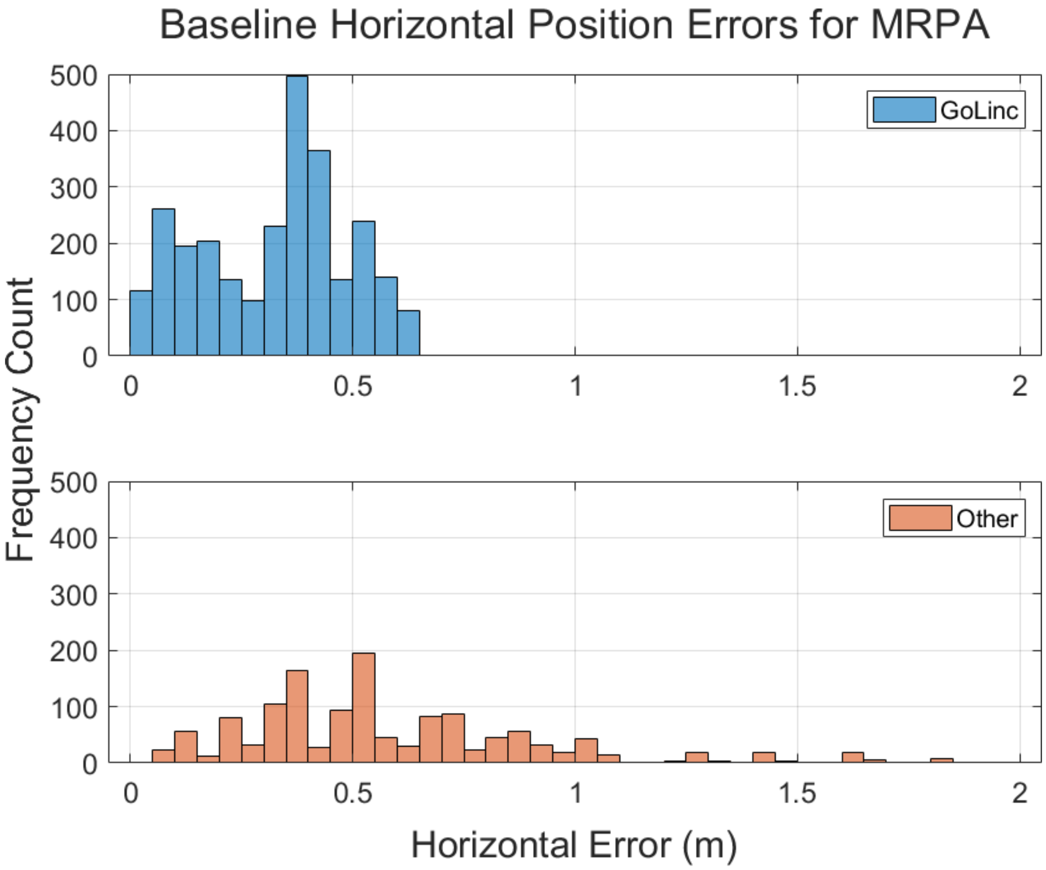


Figure 20. Comparison between two receivers of Horizontal Position Errors for MRPA

Static Response

The static response analysis investigated characteristics of horizontal position errors for each device during static scenarios. This analysis includes descriptive statistics as well as time series plots. Results are restricted to cases where a device reports position data for at least 45 seconds during the scenario, to avoid extremely low sample sizes. The 45 second threshold was found to also exclude any scenarios that had the bulk of the data points near the start and/or end of the scenario, during which times conditions are less stable while emitters transition on or off.

The following figures show descriptive statistics for the horizontal position errors of each device (horizontal axis) throughout each static scenario (vertical axis). The title of the heatmap indicates the statistic (mean vs standard deviation) as well as the location. Lower values (light yellow) indicate favorable performance. Instances without sufficient position data available (i.e. less than 45 seconds) are left blank and indicated as No Solution.

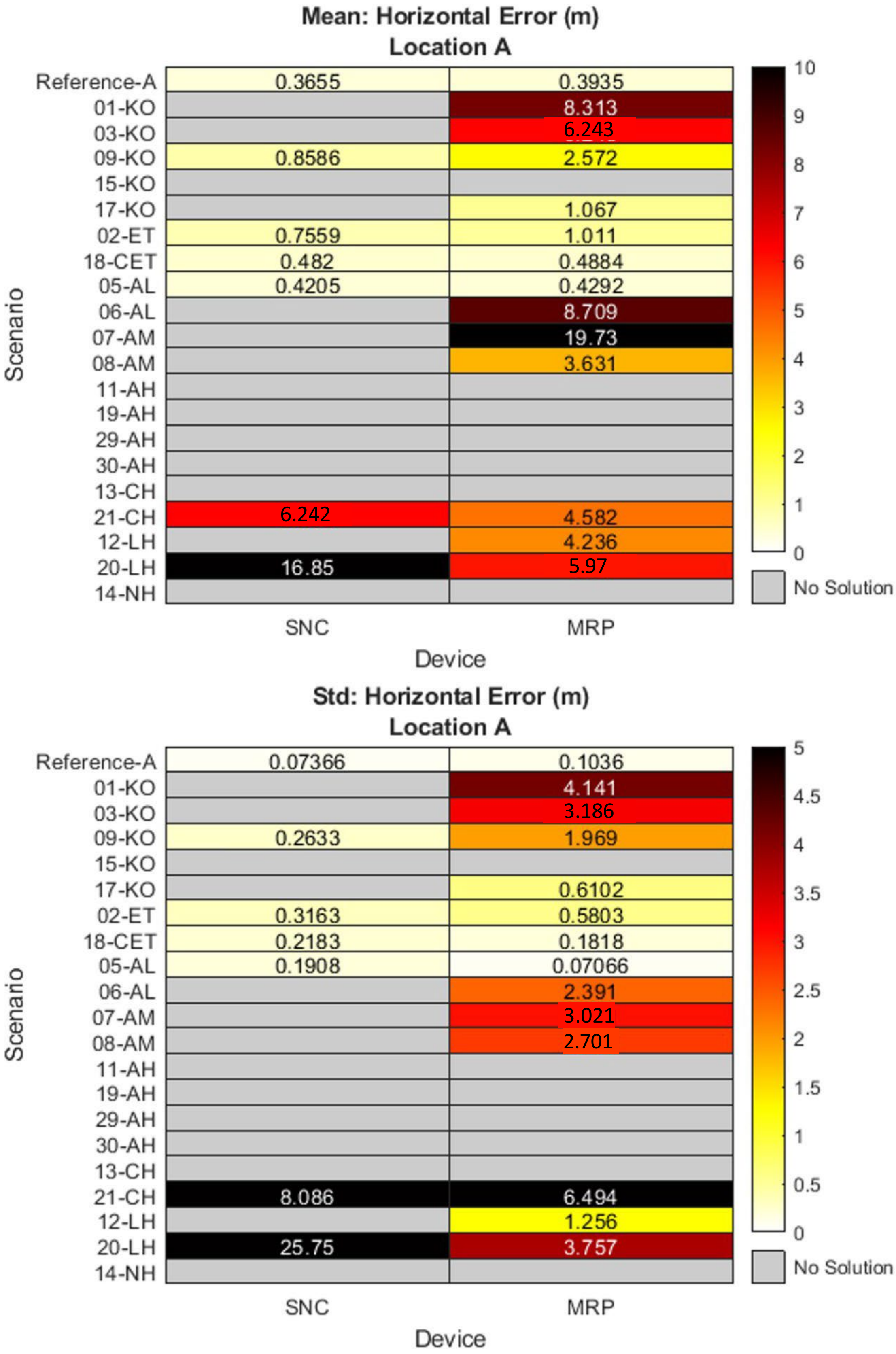


Figure 21. Heatmaps with horizontal position error statistics by device and scenario for location A

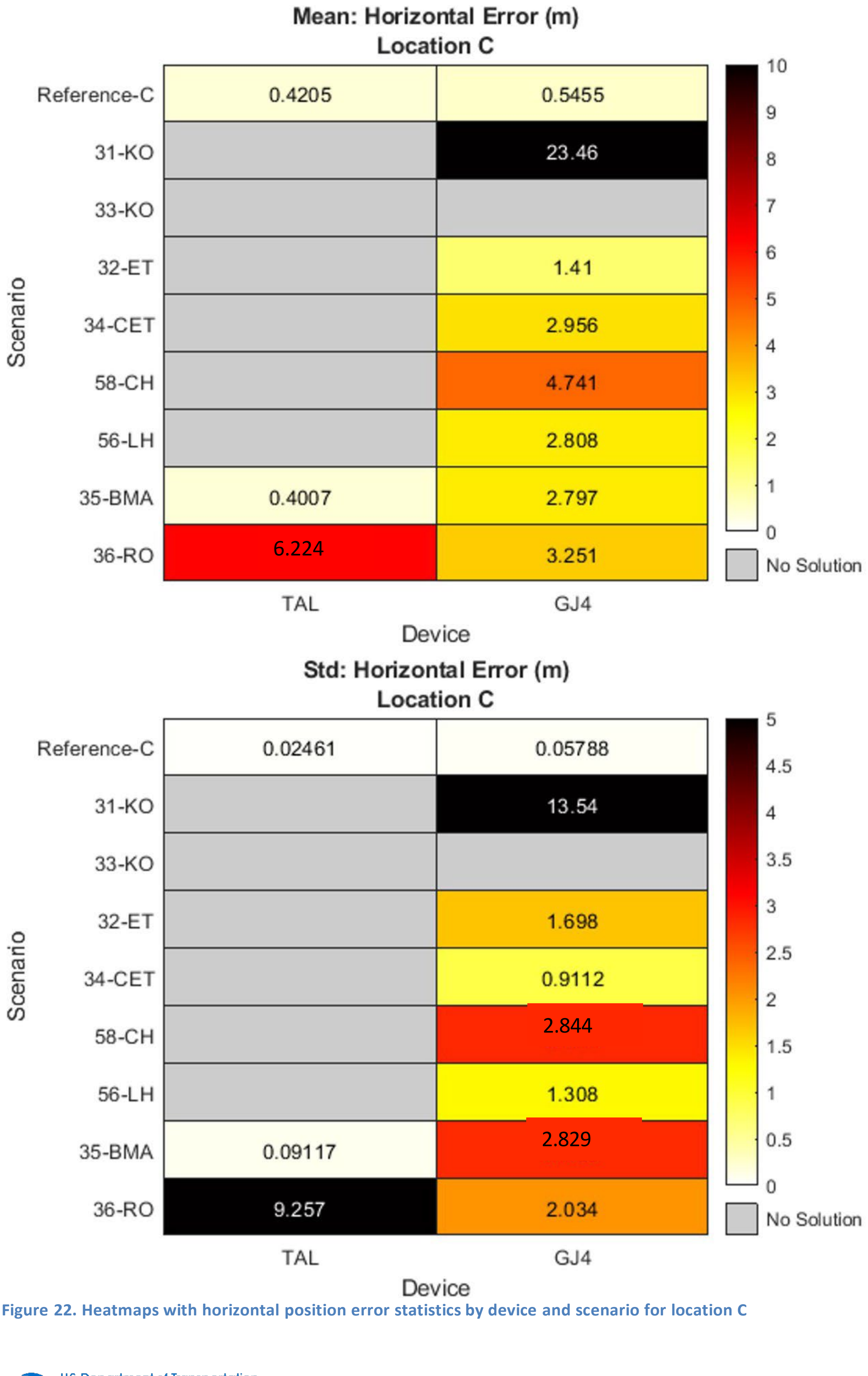


Figure 22. Heatmaps with horizontal position error statistics by device and scenario for location C

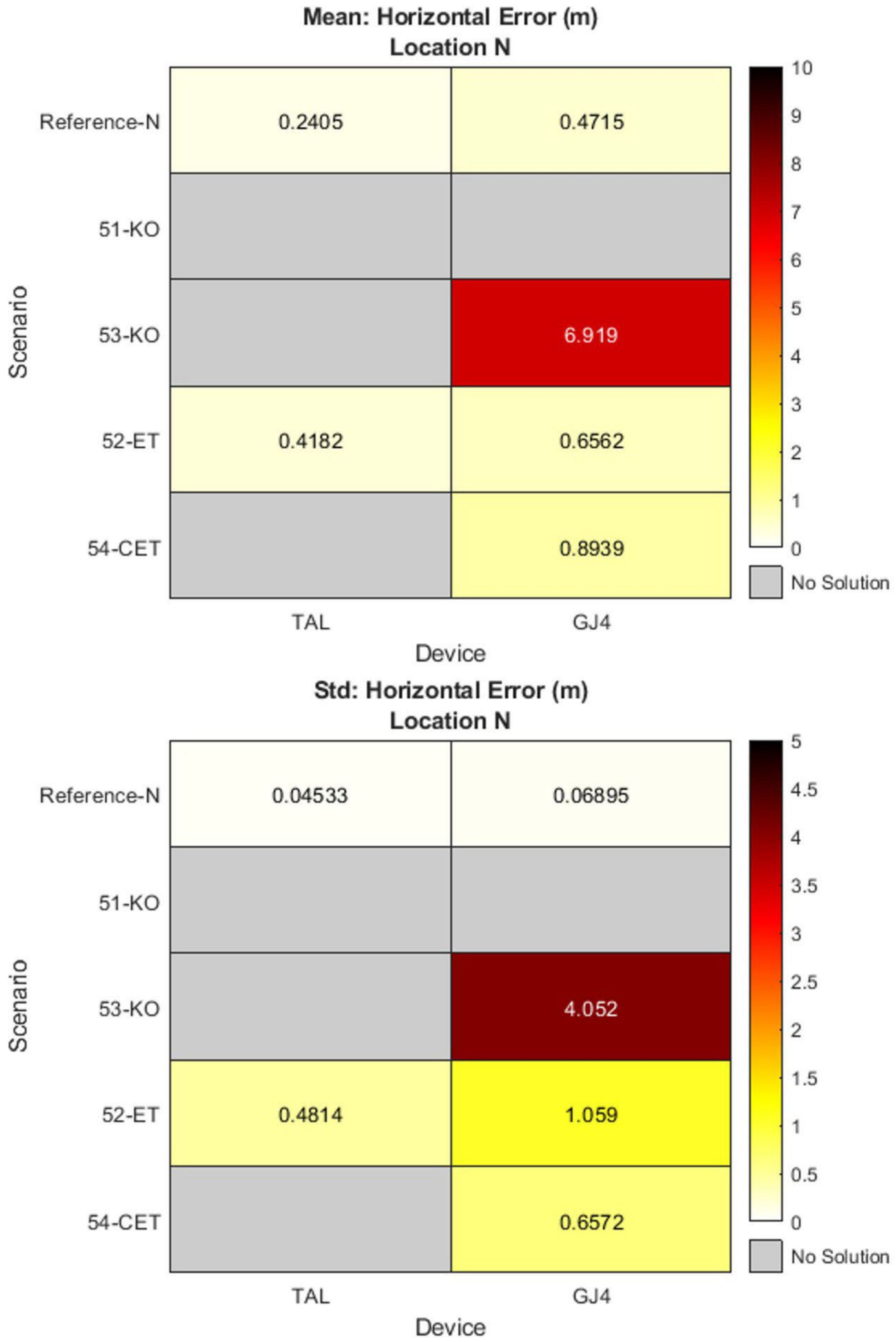


Figure 23. Heatmaps with horizontal position error statistics by device and scenario for location N

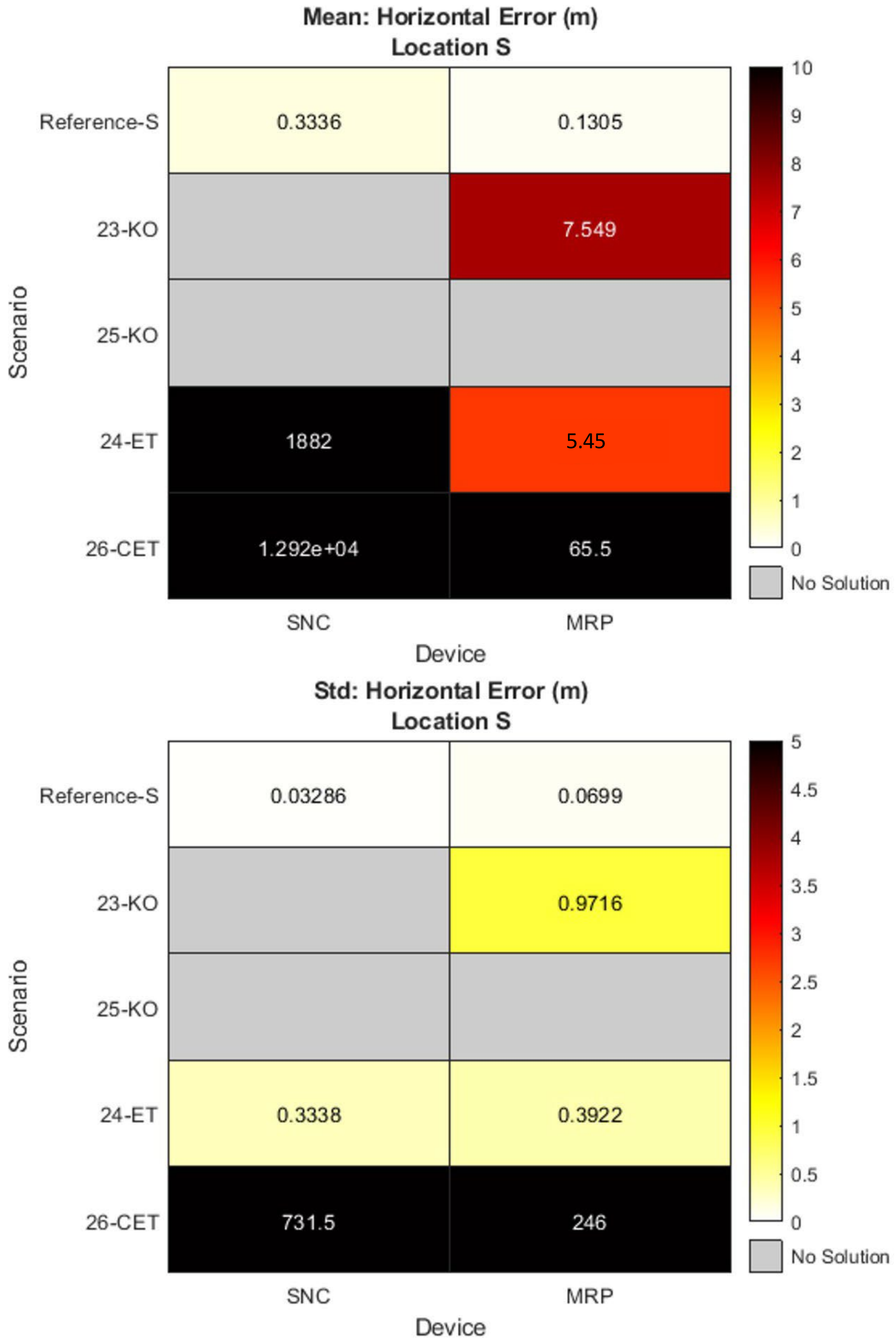


Figure 24. Heatmaps with horizontal position error statistics by device and scenario for location S

The devices show a variety of performance levels across different scenarios. Overall, the heatmaps indicate more favorable performance for the protected technologies (MRP, GJ4) over the unprotected technologies (SNC, TAL). However, there are exceptions for certain scenarios.

The heatmaps also suggest that certain devices were spoofed during two spoofing scenarios, as indicated by a large mean horizontal position error or a large standard deviation:

- 24-ET: SNC
- 26-CET: SNC, MRP

Figure 25 and Figure 26 display the horizontal position error time series during these spoofing scenarios 24-ET and 26-CET, respectively. In each figure, the top plot shows an extended view of the errors. This plot demonstrates the wide range of errors from the scale of centimeters to over 10,000 meters. The middle plot shows the same data with a focused view on errors below 5 meters. The bottom plot indicates times for which valid position data was reported for each device. Large errors indicate potential spoofing.

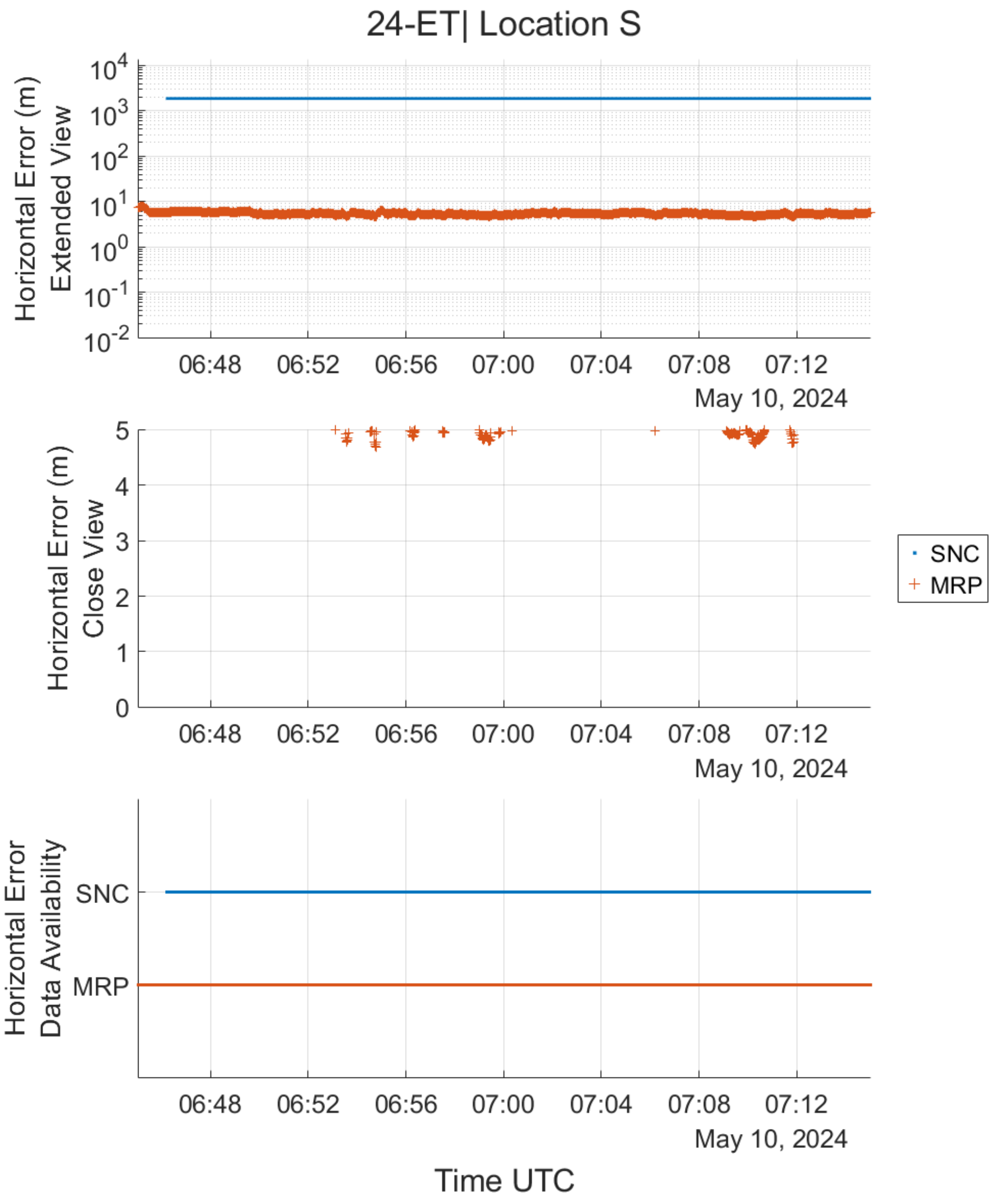


Figure 25. Time series of horizontal position errors during spoofing scenario 24-ET

The SNC consistently reports horizontal position errors above 1,000 m during scenario 24-ET, which indicates potential spoofing. The MRP consistently reports horizontal position errors below 10 m, which are above nominal baseline levels but less extreme than the errors for the SNC. The SNC appears to have been impacted more strongly than the MRP for this scenario.

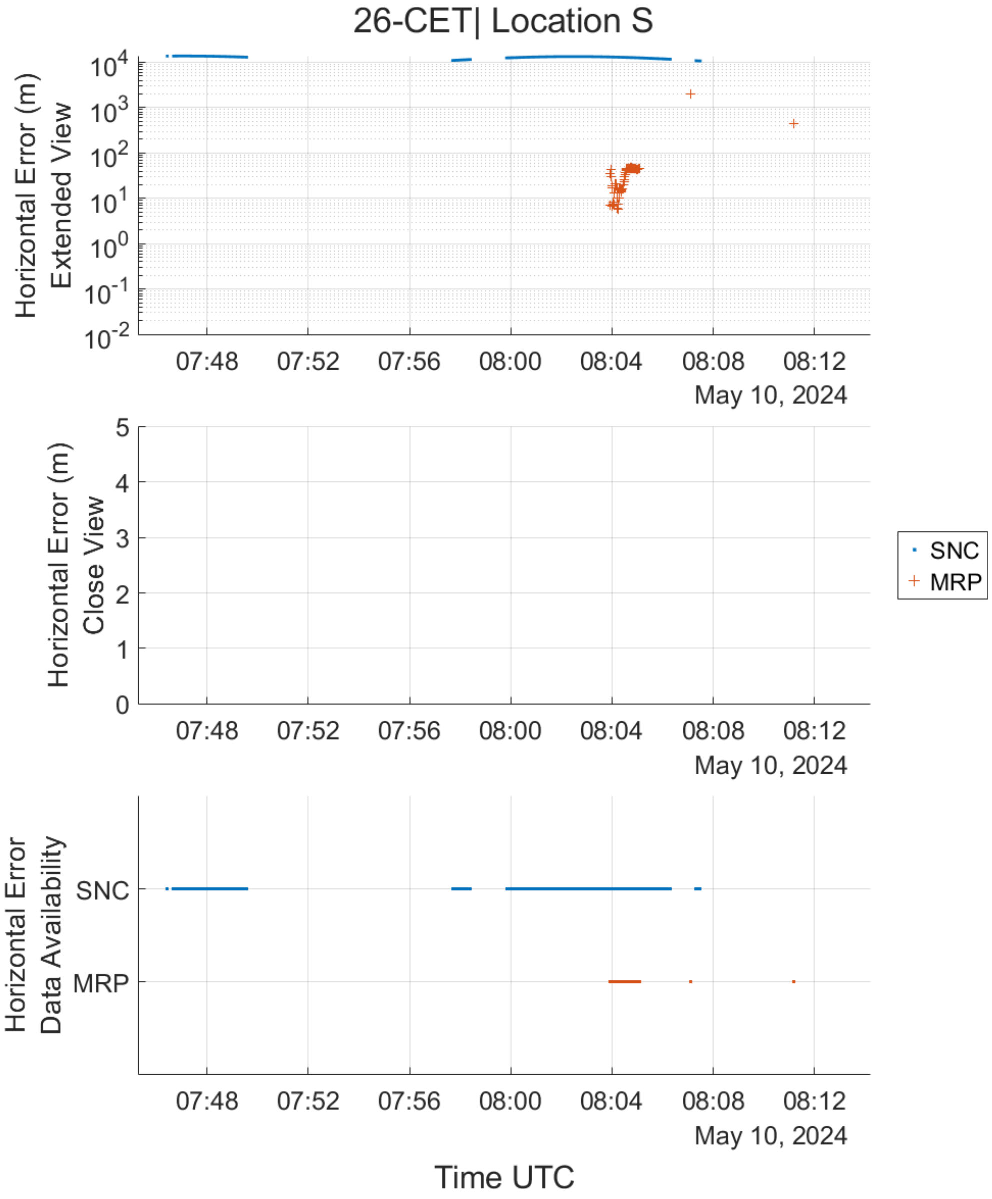


Figure 26. Time series of horizontal position errors during spoofing scenario 26-CET

The SNC reports many horizontal position errors above 10,000 m during scenario 24-ET, which indicates potential spoofing. The MRP reports many horizontal position errors across a range of values with outliers extending above 1,000 m. Both devices show disruptions in data availability. For this scenario, both devices appear to potentially be impacted by spoofing, with SNC exhibiting stronger errors than MRP.

The full set of horizontal position error time series plots for the static response analysis can be found in Appendix C: NAVFEST Static Response Analysis Time Series Plots.

The results of the static response analysis indicate an overall relative order or performance favoring the protected technologies (MRP, GJ4) over the unprotected technologies (SNC, TAL). However, there are occasional exceptions for certain scenarios.

Static Recovery

The static recovery analysis investigated the ability of each device to return to baseline performance levels after the jamming/spoofing during static scenarios had ended. This analysis was restricted to static scenarios with at least eleven minutes immediately after the scenario ended for which the van remained stationary with no interference observed, to allow sufficient time and opportunity for devices to recover to baseline performance levels. This analysis investigated recovery statistics based on recovery success vs failure, time to recovery, and recovery start condition.

5.1.1 Recovery Definition

Device performance recovery was defined based on the characteristics of the horizontal position errors over time. The horizontal errors from the static reference data sets were used to quantify the baseline performance levels. A nominal threshold representing the upper bound of baseline performance was defined for each device by scaling the 99th percentile of the reference horizontal position errors by a factor of 1.1, to avoid the influence of extreme outliers.

A recovery window is defined as the 10 minutes immediately following the end of the static jamming/spoofing scenario. A device has recovered when it reports a horizontal position error below the threshold within the recovery window and then continues to report horizontal position errors below the threshold for at least 60 seconds (i.e., the confirmation window). The device fails to recover if this condition is not met. Figure 27 demonstrates an example of device recovery.

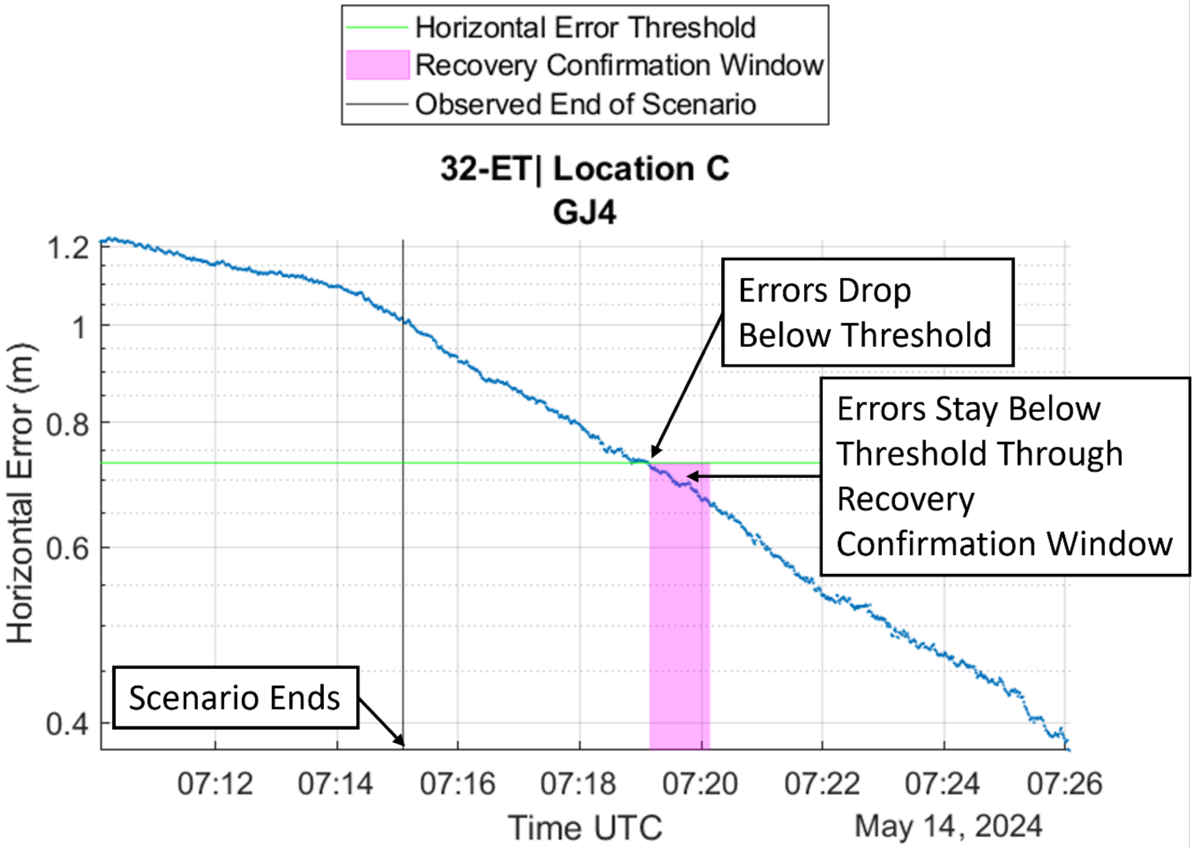


Figure 27. Time Series of horizontal position errors demonstrating performance recovery after a static spoofing scenario

The full set of time series plots for the static recovery analysis can be found in Appendix D: NAVFEST Static Recovery Analysis Time Series Plots.

5.1.2 Recovery Start Condition

The recovery start condition for a device is defined based on the horizontal position error value reported at the end of the static jamming/spoofing scenario:

- Not Reported: No horizontal position reported
- Above Nominal Threshold: Horizontal position error above threshold
- Below Nominal Threshold: Horizontal position error below threshold

Recovery start condition is an important consideration for time to recovery. For example, if a device already demonstrates baseline performance levels at the end of a scenario, there may not be any delay until it is considered recovered for this analysis (i.e., time to recovery is zero seconds). Conversely, if the device reports abnormally large errors or fails to report a position at the end of the static scenario, it may be expected to take some time to recover.

5.1.3 Static Recovery Results

Table 5 displays the number of static scenarios with no recovery for each device, grouped by recovery start condition.

Table 5. Static scenarios with failure to recover by device and start condition

Recovery Start Condition	GJ4	MRP	TAL	SNC
Above Nominal Threshold	1	2	1	2
Below Nominal Threshold	0	0	0	0
Not Reported	0	0	0	2

All devices recovered for most static jamming and spoofing scenarios. The unprotected device SNC demonstrated the most failures to recover, with four failures total. All failures to recover were investigated to assess whether a root cause could be determined. Table 6 shows a summary of the investigations.

Table 6. Root cause investigations for failures to recover

Scenario	Devices Failed	Root Cause Investigation
7-AM (jam)	SNC	Inconclusive
13-CH (jam)	SNC	Inconclusive
24-ET (spoof)	MRP, SNC	Possible explanations include the atypical proximity of the van to the emitter, or lingering effects from the spoofing signals.
29-AH (jam)	MRP, SNC	A possible explanation is that both devices showed signs of potential spoofing earlier in the same night of testing (spoofing scenarios 24-ET and 26-CET), and this may have affected their ability to recover in scenario 29-AH.
36-RO (jam)	GJ4, TAL	Inconclusive

Figure 28 shows the distribution of time to recovery for each device. The start condition for each data point is indicated by color, as labeled in the legend.

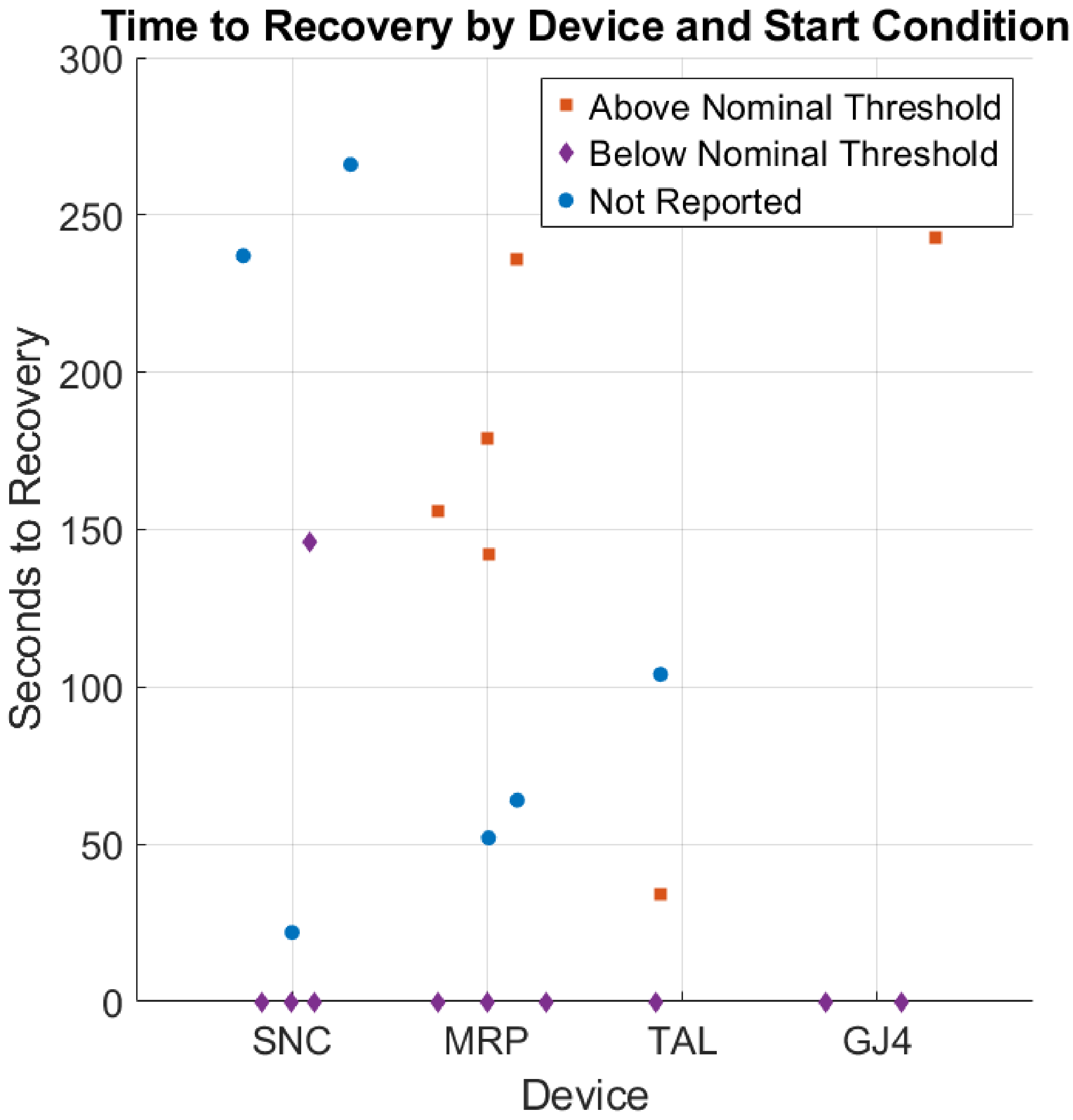


Figure 28. Time to recovery distributions for each device

Most devices demonstrate a range of times to recovery, spanning from zero seconds (immediate recovery, often with start conditions already below nominal threshold) to several minutes. As a reminder, the devices were tested in pairs (SNC vs MRP, TAL vs GJ4). Due to constraints for the sample sizes and types of scenarios involved for each device in the static recovery analysis, it is recommended to compare SNC directly with MRP and to compare TAL directly with GJ4.

The static recovery analysis indicates that, overall, each device pair demonstrates subtle differences in the distributions of time to recover without any overwhelming advantage for either device. However, the SNC experienced the most failures to recover, with twice as many failures as the MRP.

NAVFEST Conclusions

In general, the results of the NAVFEST data analysis indicated a relative overall order of device performance under a variety of spoofing and jamming conditions, though exceptions occasionally occurred for certain performance criteria in certain scenarios. The protected technologies (MRP, GJ4) typically showed favorable performance over the unprotected technologies (SNC, TAL). This is consistent with expectations based on the sophistication of the protection technologies. For example, antennas with more elements are expected to provide greater protection than antennas with fewer elements.

6. Complementary PNT for Rail

Amtrak has stated dead reckoning as a primary PNT challenge. Amtrak trains must obtain PNT solutions in GNSS-challenged environments in order to operate safely and reliably through these environments. Examples include underground and covered stations, urban and natural canyons, and tunnels.

Within the NEC, Amtrak utilizes the second generation of the Advanced Civil Speed Enforcement System (ACSES II) for PTC.[34] ACSES II is a balise-based system described in further detail in Appendix A. For Amtrak, ACSES II is limited to the rail lines it owns (primarily the NEC, depicted in Figure 29). Passenger train operations across rail lines owned by freight operators must utilize I-ETMS for interoperability, with which ACSES II is incompatible. Discussions with the freight rail industry revealed their unwillingness to adopt ACSES II, as it would not scale to the thousands of miles of rail lines outside of the NEC. For this reason, Amtrak's Dead Reckoning outside of the NEC relies upon wheel tachometers,[35] which are prone to drift and error that accumulate over time and distance.

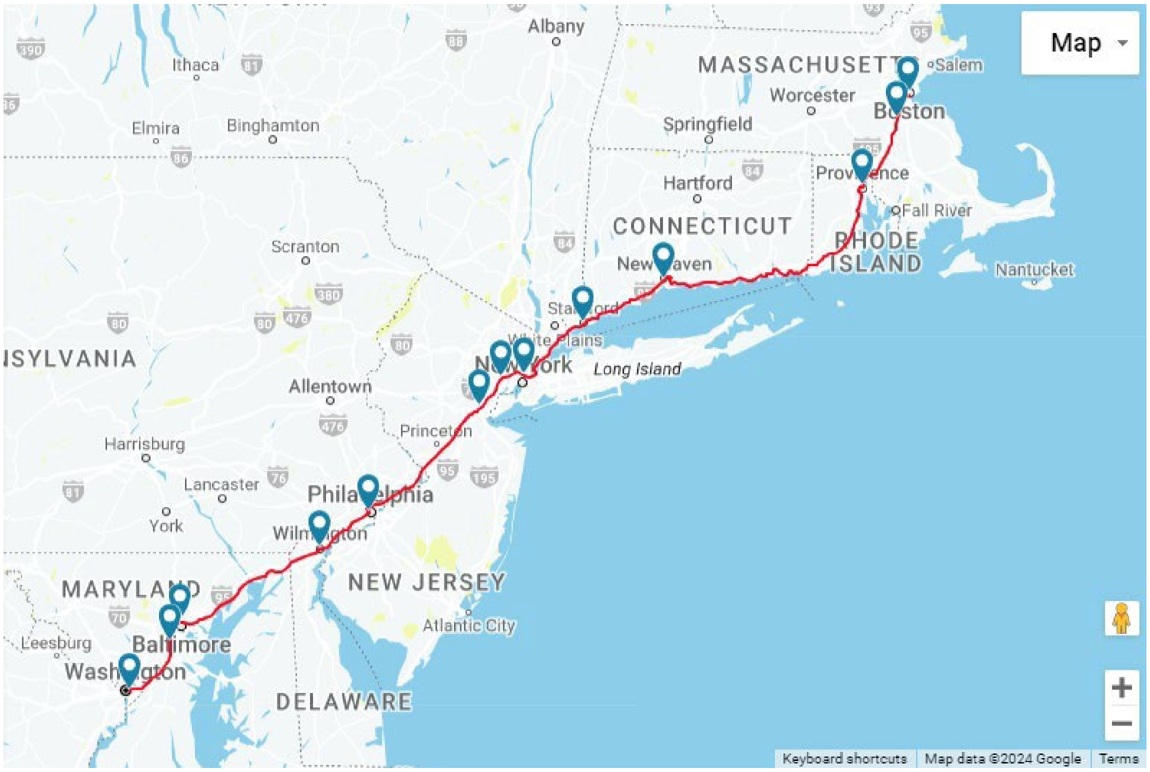


Figure 29. Map of Amtrak's Acela service in the Northeast Corridor[36]

Amtrak's GNSS-denied operations are subsequently limited in the distance that can be safely traveled from the point of GNSS signal loss. Amtrak and the freight rail industry conveyed their interest in the following CPNT technologies for improved dead reckoning operations. The fundamental basis for each candidate is locomotive-mounted front-end sensor data to determine train position relative to known track points of interest (TPOIs).

Sensor Fusion

Though not a CPNT source in its own rite, fusion of multiple PNT sources such as inertial measurement unit (IMU) and magnetometer potentially provides a PNT capability through intelligent integration of GNSS signals and inputs from other sources. Sensor Fusion potentially includes processing of GNSS-based logging of the detection of jamming and spoofing by receivers so equipped.

The Wabtec PNMs possess built-in sensor fusion. However, this feature is not presently implemented. There exists an IMU + magnetometer capability, which is not yet enabled on Amtrak trains. Future CPNT testing should consider sensor fusion, with the aim of enhanced dead reckoning per AAR specifications.[37]

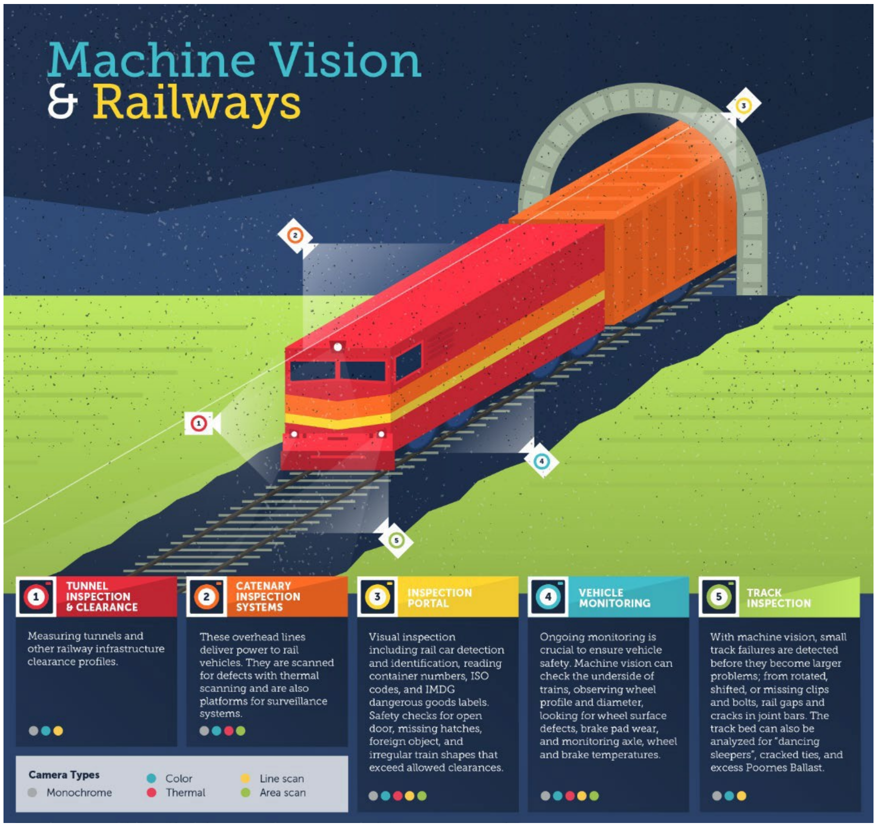
Machine Vision

Deep or machine learning based on Artificial Intelligence (AI) processes data from real-time cameras mounted on trains. AI provides complex interpretation to aid the speed and accuracy of feature-matching imagery of the train's surroundings to various map databases. The purported accuracy of Machine Vision is under 5 meters.

A powerful enabling technology, AI-based deep/machine learning is an increasingly important tool in enabling sensor fusion to reach its full potential, particularly regarding visual sensor data which requires complex interpretation. Skyline Nav AI has developed proprietary technology which fuses visual sensor data, AI and digital elevation maps (DEM) and developed algorithms to recognize skyline/horizon features. This capability has been tested in feature rich as well as sparse settings and demonstrated the capability to perform geolocation, even with limited field of view. Another proprietary solution, Visual Positioning System (VPS) from Brooklyn-based Vermeer, leverages AI and full motion video (FMV). VPS employs a global geo-rectified 3D map database that feature-matches the platform's FMV feed. VPS software is sensor and system agnostic; it can be applied to an existing vehicle/fleet and can work in conjunction with GPS and other CPNT sources, or on its own.

The primary advantage of Machine Vision is its RF independence. This technology is inherently immune to GNSS interference of all types, potentially providing full functionality in GNSS-limited or -denied environments. This technology may also function as a GNSS resiliency complement, dead reckoning calibration source, or backup navigation system. Machine Vision may utilize various frequencies and bandwidths of differing characteristics, i.e., the strengths of one balancing the weakness(es) of others, in challenging weather and ambient lighting conditions.

A key disadvantage is that systems operating in the visual range may not be suitable for all weather conditions, especially where visibility is reduced. Nighttime performance will also be degraded, depending on ambient conditions. Featureless environments may also be problematic. Current usefulness may be limited in cases where image data includes near-field obstructions to the horizon, skyline, or permanent features. Additionally, availability could be limited by gaps in input data, e.g., gaps in reference mapping databases or deficiencies in image matching algorithms.



Measuring tunnels and other railway infrastructure clearance profiles.

These overhead lines deliver power to rail vehicles. They are scanned for defects with thermal scanning and are also platforms for surveillance systems.

Visual inspection including rail car detection and identification, reading container numbers, ISO codes, and IMDG dangerous goods labels. Safety checks for open door, missing hatches, foreign object, and irregular train shapes that exceed allowed clearances.

Ongoing monitoring is crucial to ensure vehicle safety. Machine vision can check the underside of trains, observing wheel profile and diameter, looking for wheel surface defects, brake pad wear, and monitoring axle, wheel and brake temperatures.

With machine vision, small track failures are detected before they become larger problems; from rotated, shifted, or missing clips and bolts, rail gaps and cracks in joint bars. The track bed can also be analyzed for "dancing sleepers", cracked ties, and excess Poornes Ballast.

Figure 30: Current Rail Use Cases for Machine Vision[38]

The largest impediment to Machine Vision adoption is its low Technology Readiness Level (TRL) in a PNT application. Image processing algorithms are computationally intensive, requiring significant computational resources.[39] Such resources are beyond the capability of real-time on-board image processing for a train in motion. Finally, featureless environments may be difficult to match to an on-board database.

Ground Penetrating Radar

Ground Penetrating Radar (GPR), first developed over twenty years ago, has largely been used in niche applications such as archaeology, structural engineering assessment, and utility location. However, due to GPR's unique capabilities to identify underground features, it has gained significant traction as a source of complementary PNT over the last decade. To date, Amtrak and other rail operators employ this technology for track inspections,[40] as depicted in Figure 31.

GPR systems work by sending a pulse of electromagnetic radiation into the ground and measuring reflections that originate from scattering below the surface. Reflections occur at the boundaries between objects of different electromagnetic properties, e.g., the interfaces between soil and rocks, roots, or man-made features. GPR sensor data in conjunction with AI-enhanced software can create a detailed image of the subsurface environment. Nearly all discrete objects and soil features are captured if they are not significantly smaller than the wavelength of the radar employed and that there is sufficient dielectric contrast with the surrounding soil. The premise of GPR localization is that these subsurface features, as represented in GPR data, are sufficiently unique, permanent, and impervious to environmental phenomena (such as snow and fog) to permit their use as identifiers of the precise location where they were collected. GPR, like other technologies, may be enhanced through fusion with GNSS and other CPNT sources.

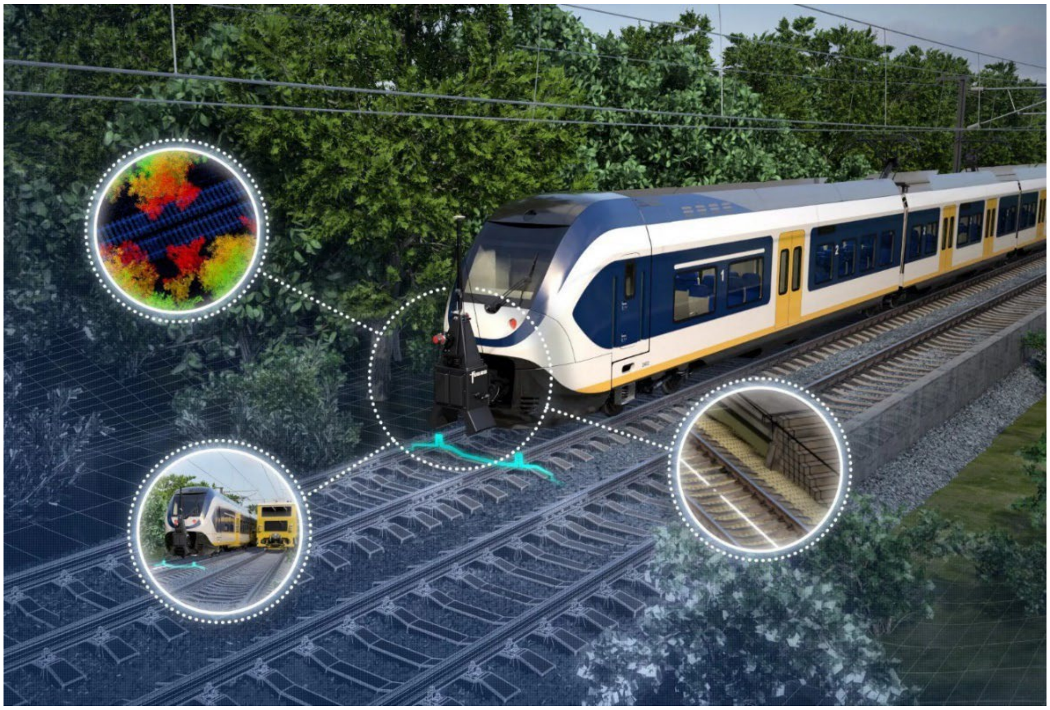


Figure 31: Current Rail Application for Ground Penetrating Radar[41]

GPR penetration may not be possible in certain types of unique terrain, on metal bridges or similar surfaces. GPR cannot tell the composition of a target; it can only tell if there is a contrast between the target and the surrounding area. Water reflects the signals differently from materials in the ground, which can mask the presence of utility lines or other objects of interest. The RF conductivity of the ground, the RF frequency utilized, and the power of the RF emitter all limit the depth of imaging on the order of 2-10 feet.

Similar to Machine Vision, the largest impediment to adoption is its low Technology Readiness Level (TRL) in a PNT application. Radar data processing is likewise computationally intensive, requiring significant computational resources, e.g. 50 miles of raw data from GPR requiring 8 hours of post-processing. As discussed with federal and industry partners, GPR, in its present state of maturity, is beyond the capability of real-time on-board data processing for a train in motion.

Ultra Wide Band

Ultra Wide Band (UWB) ranging can be used stand-alone or as a sensor fusion input to support PNT solutions. UWB technology operates on unlicensed 7.5 GHz RF spectrum (3.1 – 10.6 GHz) and can transmit through various mediums such as air or the ground.[42] UWB ranging transmits between two (or more) devices to determine the distance between the devices and typically utilizes Time-Of-Arrival (TOA) methods to determine the Line of Sight (LOS) path between devices. The advantages of UWB include low power requirements, low probability of interference, large bandwidth for multitudes of signals, and high accuracy for timing and positioning.

The primary disadvantage of this technology is limited range; use is typically limited to ~50 meters due to the low power signals. Initial infrastructure requirements such as complex antenna configurations and precise calibrations are also an important consideration. Applications for rail were previously believed unlikely due to range limitations, however a UWB hybrid system has been developed to transmit time and position from GPS advantaged positions to remote nodes. Furthermore, Amtrak is investigating this technology for Dead Reckoning applications.[43] Other possible rail applications include shorter-range use cases, such as rail terminals and underground stations where GPS is often unavailable, but high precision timing and positioning are required.[44]

7. Conclusions and Recommendations

The U.S. DOT's Pilot Program has produced significant achievements in all four components that EO 13905 specifies for improving operational resilience through responsible use of PNT. As identified in EO 13905, PNT profiles are intended to:

- Enable the public and private sectors to identify systems, networks, and assets dependent on PNT services;
- Identify appropriate PNT services;
- Detect the disruption and manipulation of PNT services; and
- Manage the associated risks to the systems, networks, and assets dependent on PNT services.

The FRA Pilot Program focused on GNSS equipment for passenger rail in the U.S. and provided findings and recommendations along each of the four components by:

1. Partnering with Amtrak as the use case for this program, through industry discussions and given the applicability of EO 13905 to the Rail Mode.
2. Identifying specific passenger rail GNSS equipment through industry outreach and study of Amtrak trains.
3. Detecting the disruption and manipulation of GNSS service through successful testing of rail PNT equipment in "live sky" normal and disrupted/manipulated conditions. The primary evaluation in the study leveraged NAVFEST as the environment for testing identified GNSS equipment with and without added protective capability.
4. Identifying both existing and complementary PNT data sources that are suitable for the rail operating environment through industry outreach, literature search, and discussion with project partners.

The basis for the Pilot Program was the NIST Foundational PNT Profile specified in NISTIR 8323. As a Pilot Program, the team sought to develop actionable areas for increasing the PNT resilience of trains. The central findings from the Program team were developed through the five NISTIR 8323 Framework Core functions. Addressing those five functions led to three actionable fronts for managing operational risk from PNT disruption and/or manipulation:

1. Know your risks;
2. Protect your systems; and
3. Incorporate diversified sources of PNT signals.

In alignment with the actionable objective of the Pilot Program, the findings above are suitable for application in passenger rail service and should be considered as capabilities that can be incorporated into a system solution for satisfying GNSS resiliency requirements. Protective and diversifying solutions are effective and commercially available. The results provided in Section 5 demonstrate that these solutions should be further evaluated with respect to the full set of operational requirements for a platform such as an Amtrak locomotive. However, from the PNT Profile perspective, the U.S. DOT Pilot Program findings lead to two recommendations for improving PNT resilience.

1. Protect existing or new GNSS equipment on passenger trains with controlled reception pattern antenna (CRPA) technology. Solutions such as the Hexagon GAJT-410ML can protect GPS-derived PNT outputs, with no further changes needed to on-board equipment. When paired with the GAJT nulling antenna, the GoLinc PNM receiver will be unable to demodulate the spoofing data therefore protecting the receiver from the vast majority of both signal and data spoofing attacks. This solution, if desired, does have the capability to serve also in a detect-and-characterize function (power and direction of arrival) on interfering signals. Further, a dual antenna/receiver pair can be used to detect a spoofing attack through self-differential means. (A concept under study by the industry proposes a GNSS antenna-receiver set installed at each end of a train, and could potentially also furnish this spoofing attack detection capability.)
2. Augment GNSS with CPNT. Solutions such as ACSES currently provide a complementary PNT source for train positioning. However, as noted in Section 6, sensor fusion is not yet enabled on board passenger trains. Further, ACSES is limited to the NEC and is not deployable across the I-ETMS systems of nationwide rail networks.

Given the current interest in the rail sector for CPNT technologies over those for GNSS, protective solution cost is an additional consideration. Thus, a business case analysis must be made for investment in protective GNSS solutions vice CPNT technologies.

While these recommendations are tailored to the focused work of rail GNSS, operational impact findings will potentially give a greater indication that such protect-and-diversify solutions are likely applicable to a much wider cross-section of passenger train operations and locations. Thus the U.S. DOT Pilot Program can serve both as an early pathfinder for PNT resilience in passenger rail and as a template for effective application of PNT resilience to many operational rail environments. Additionally, project findings could inform future FRA rulemaking regarding PTC and its PNT requirements.

8. Planning for the Next Phase

Fulfillment of the 5 functions of the NIST PNT Profile, detailed in Section 0, requires continuation of this effort into a second phase. The results of the current effort fully complete the Identify function, and partially complete the Protect and Detect functions, but did not include the Respond and Recover functions.

The primary focus of Phase 2 will be operational GNSS testing. That is, the equipment tested at NAVFEST (see Section 4) will be installed on a rail test vehicle for evaluation in an operating environment. The results of this testing will yield more definitive conclusions about GNSS resiliency options for rail. Ideally, test equipment installation would take place on board an Amtrak train in regular passenger service.

A radio frequency (RF) survey will also be conducted on a test train. This report will consider planning for this exercise.

Test Setting

Amtrak and FRA preliminary planning with the Volpe team indicates an Amtrak passenger train operating along the NEC as the preferred test setting. The NEC provides an operationally-relevant, inherently demanding RF environment. Amtrak further expressed the utility of executing the RF survey in the NEC to inform next-generation PTC integration in that section of the Amtrak network. Expected sources of train-based interference include on-board radios, diesel engines, electric traction motors, and catenaries providing electric power from overhead lines.

Should testing directly on an operational Amtrak rail line prove impractical, two options exist for on-board rail testing. The Transportation Technology Center (TTC) in Pueblo, CO offers rail research and testing (both on-track, and in laboratories) and associated engineering services. The TTC encompasses a 52 square mile facility (depicted in Figure 32) with over 50 miles of track containing both wayside and on-board PTC equipment, with a railcar available for GNSS equipment installation. The TTC is operated by ENSCO under a “care, custody, control contract” with FRA, with provisions for Volpe Center utilization.

FRA offers an additional option through its Automated Track Inspection Program (ATIP). ATIP utilizes multiple cars for track inspection, including autonomous box cars as well as rail-usable cars. Some of the cars in ATIP already have GNSS equipment installed and operating, facilitating their use in this project. As illustrated in Figure 33, ATIP cars possess ample rooftop area for equipment installation. However, FRA indicated that this railcar lacks the RFI environment of an operational passenger train, making ATIP an unfavorable testbed. Likewise, the remoteness of the TTC means a far more benign RF environment than the more densely populated areas through which the NEC runs.

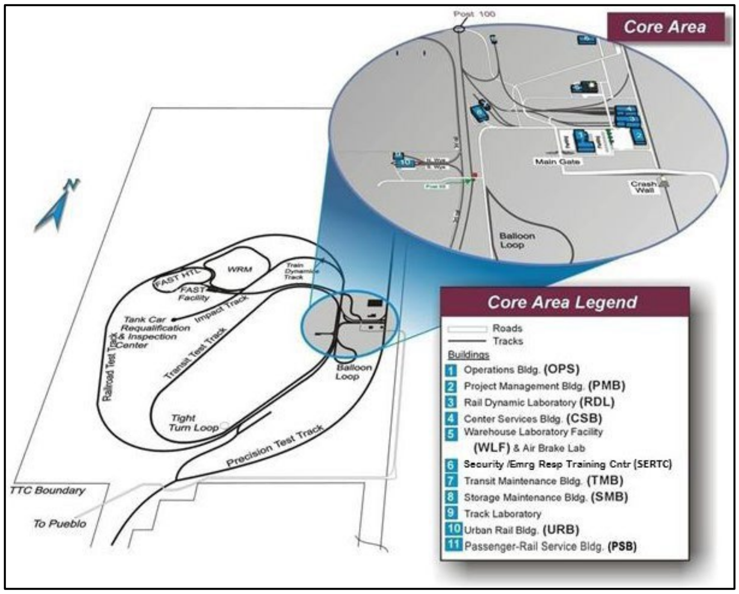

Post 100
Core Area
Main Gate
Crash Wall
Balloon Loop
FAST HTL
WRM
FAST Facility
Train Dynamics Track
Tank Car Requalification & Inspection Center
Impact Track
Railroad Test Track
Transit Test Track
Balloon Loop
Tight Turn Loop
Precision Test Track
TTC Boundary
To Pueblo
Core Area Legend
Roads
Tracks
Buildings
1 Operations Bldg. (OPS)
2 Project Management Bldg. (PMB)
3 Rail Dynamic Laboratory (RDL)
4 Center Services Bldg. (CSB)
5 Warehouse Laboratory Facility (WLF) & Air Brake Lab
6 Security /Emrg Resp Training Cntr (SERTC)
7 Transit Maintenance Bldg. (TMB)
8 Storage Maintenance Bldg. (SMB)
9 Track Laboratory
10 Urban Rail Bldg. (URB)
11 Passenger-Rail Service Bldg. (PSB)

Figure 32: Map and Overview of TTC[45]

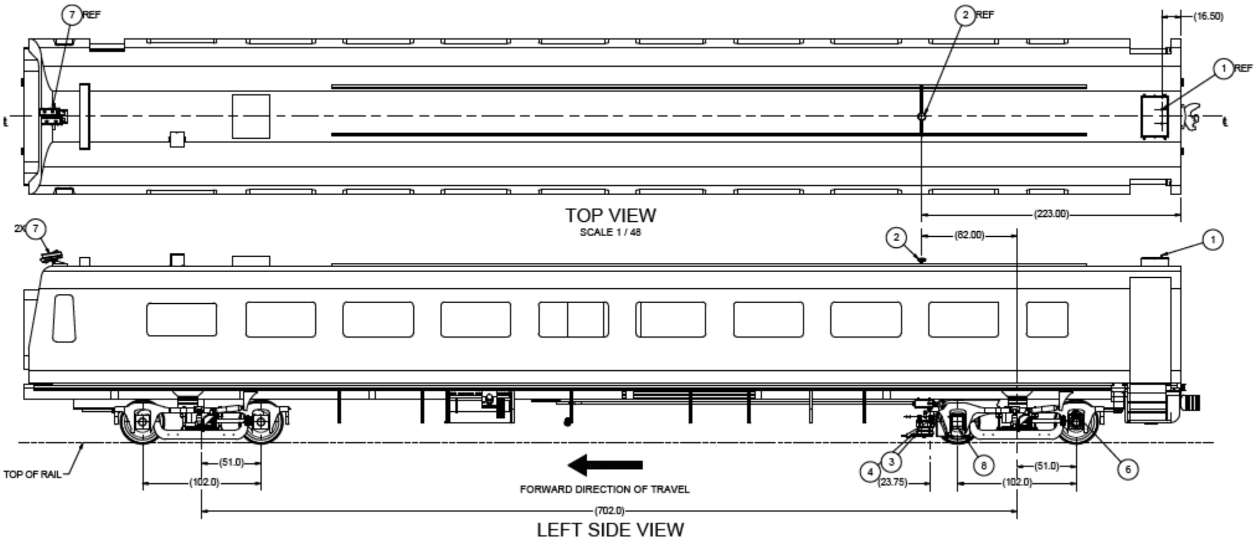


Figure 33: Profile of FRA ATIP car[46]

As a result, Amtrak's Siemens ACS-64 locomotive operating in the NEC provides the preferred equipment and setting for operational testing and the RF Survey. The ACS-64, shown in Figure 34, powers Amtrak's Northeast Regional and long-distance trains on the NEC mainline, as well as other rail branches.[47]

Figure 34: Amtrak ACS-64 Locomotive undergoing pre-delivery testing at the TTC[48]

PNT Equipment

In addition to previously tested equipment, operational testing may include additional candidates for GNSS jamming and spoofing mitigation. First, candidate receivers beyond the Wabtec/Septentrio equipment discussed may be found through further market research and additional discussions with rail operators.

Second, additional protective antennas may be considered; one example is the Tualcom 3300D depicted in Figure 35. This antenna, a marine-hardened GNSS CRPA, has been specifically designed to deliver the maximum possible protection within ITAR limits. [49] That is, the antenna is ITAR-clear, given its 3 antenna elements and 30-35dB null depth. The 330D can provide protection in the L1, L2, and L5 bands against 2 simultaneous jamming sources.

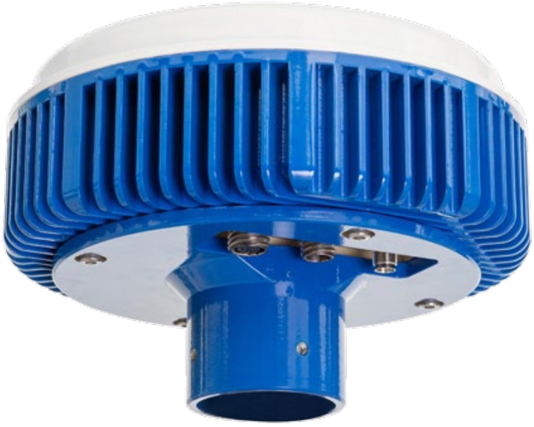


Figure 35: Tualcom 330D ITAR-Clear CRPA

In addition to CRPAs, other articles offer GNSS protection. The Infinidome OtoSphere, shown in Figure 36, is a commercially available anti-jam and anti-spoof device. The OtoSphere provides jamming protection in the GPS L1 C/A band while passing through GLONASS and GPS L5 frequencies. The OtoSphere is installed in-line between any commercially available GNSS receiver, and any two identical GNSS antennas. The OtoSphere is IP67-rated and can be installed inside a protective case or within a vehicle interior.

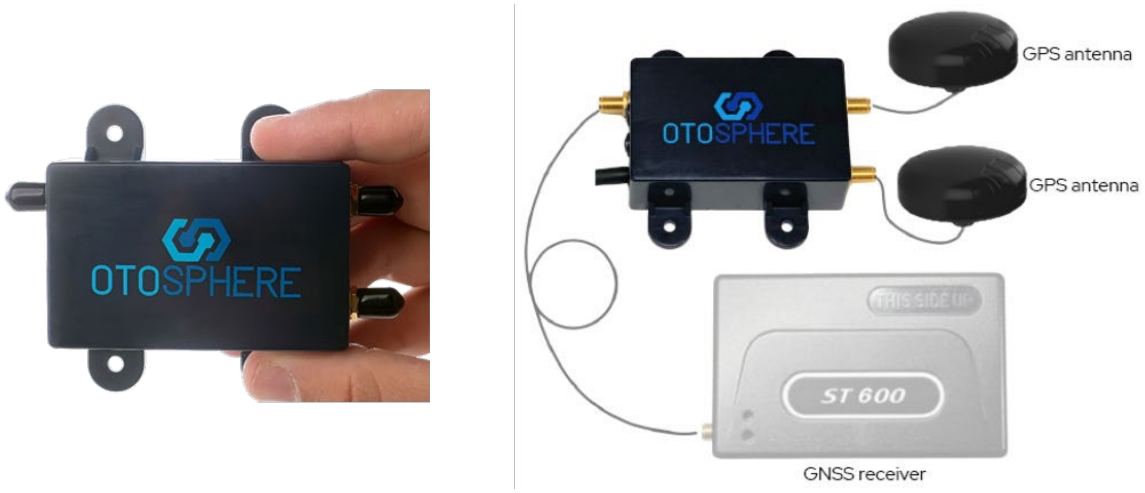


Figure 36: Infinidome OtoSphere: relative size (left) and schematic of installation (right)

One note of caution is the more restrictive tunnel heights of the proposed NEC setting for the survey. This may eliminate some of the feasible antenna candidates.

RF Survey

Unintentional environmental factors can affect the performance of on- and off-board PNT sources including GNSS as well as certain complementary technologies. For example, the Volpe Team's experience with the MARAD pilot project discovered interference of an unknown origin in the GPS L5 band both from shore and at sea. In addition, interference from an onboard system was observed in the GPS L1 band, as depicted by effects on position and signals tracked in Figure 37. The next phase of this project will seek to determine similar sources of PNT interference to rail in operation.

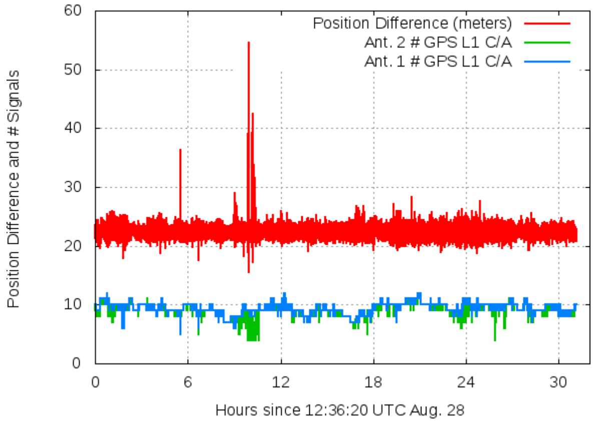


Figure 37: Effects of GPS L1 Interference detected in MARAD Pilot Project

In particular, GPS and other RF-based PNT systems can suffer from signal degradation due to interference from other devices installed on a train and from other RF transmissions in a train's operational environment, especially if such transmissions generate integer harmonics in the passband of the L1 reception band. GPS-based PNT solutions can also be significantly degraded due to satellite signal blockages, or multipath effects caused by objects and structures aboard or around the train. To understand and quantify the impact on current PNT systems and assess the effectiveness of protective and complementary technologies, a detailed assessment of the RF environment would be performed onboard a train operating on a track.

To identify these threats, the RF environment aboard an operating Amtrak train will be analyzed to characterize the existing frequency ecosystem. GNSS measurement and positioning performance will be evaluated from data collected on the selected train. The technical team will perform a radio frequency (RF) and GPS measurement survey to characterize emissions and GPS performance in a typical rail operational environment. The purpose of this evaluation is to provide insight on typical GPS performance in the rail environment, in support of recommendations being developed to improve PNT resiliency.

Certain radio bands, including those near the GPS L5 band, will be of particular interest in the RF survey. Additionally, FRA and Amtrak shared that an unknown company is planning to utilize a band adjacent to their communications bands. The frequencies of interest are 900 MHz and 928 MHz. The 900 band was previously allocated as a PTC departure test server; however, it was not used because it was subject to interference. This has since been set to 217-223 MHz, the primary band for PTC. 900 MHz is also used by freight rail for inter-car communications. The 928 MHz is allocated to FRA and Amtrak but presently not in use.

A survey system will be installed on the selected train to capture RF spectrum transmissions in and near the GPS bands (L1, L2, and L5) and to collect GPS measurement data. The GPS spectral data will be inspected to determine emitters close to the GPS band, while wider-band spectral data is expected to reveal potential RF spectrum conflicts with PNT technologies and other existing systems. GPS collection will enable characterization of the selected train's multipath conditions and provide data useful for investigating onboard GPS interference.

The survey system will utilize Volpe's prior MARAD PNT work, comprised of equipment to capture RF spectrum in and near the GPS bands (L1, L2, and L5) and to collect GPS measurement data. The main items for the survey system include:

- RF and digital electronics for sweeping GPS frequency bands,
- RF switches routing signals from many antennas,
- A dual GPS receiver (multi-frequency, multi-constellation GNSS receiver) with an internal inertial measurement unit (IMU), and
- Laptop computers for control and data collection under software control.

The components of the survey system are depicted in Figure 38. All equipment is planned to be located in the engineer's cab of the locomotive. The dashed line indicates devices that will be enclosed together in equipment cases installed onboard the locomotive.

A Signal Hound Spectrum Analyzer will process RF frequencies, sweeping the range 1.0–2.5 GHz from a single omnidirectional antenna, and RF within the GPS L1, L2, and L5 frequency bands from up to six directional antennas and a second omnidirectional antenna. The RF for the wider span collection (the "Wide-Span Survey") will use a simple passive antenna, while the RF collection for GPS L1, L2, and L5 (the "GPS-Band Survey") will filter the bands of interest and amplify them. The spectrum analyzer will source RF from these antennas sequentially via RF switches. The GNSS data collection will be conducted utilizing the PwrPak7 (see Section 4), as it is a dual antenna receiver that can support the front and rear antennas described. For PNM data, the test setup would split antenna feeds to both PwrPak7 and two PNMs. (Two PNM are needed to gather data such as train heading; the data would then need combining.) The proposed antennas are anticipated to meet the more stringent roof clearance requirements for locomotives operating along the NEC.

The survey system components will be installed in a combination of locations, pending a site survey:

- on the roof of the locomotive (see Figure 39 and Figure 40);
- inside the engineer's cab of the locomotive; and
- on an adjacent passenger car.

The two GPS antennas will be located at the fore and aft extremes of the locomotive roof to maximize their baseline separation. The omnidirectional antenna for the wide-span survey passive RF collection will be attached at a practical and permissible location.

Cases for the omni and directional antennas will be secured along the rear of the locomotive. The locomotive site survey may reveal adequate space for existing antenna cases used in the MARAD effort. If so, the two larger cases will contain three directional antennas to provide six-sector antenna coverage of the L1, L2, and L5 GPS bands. The smaller case will have one omnidirectional antenna mounted on top, and the high-speed RF switch and the L1, L2, and L5 filter/amplifier mounted inside. If space is more constrained, substitute multi-element antennas cases will be developed to fit within available space.

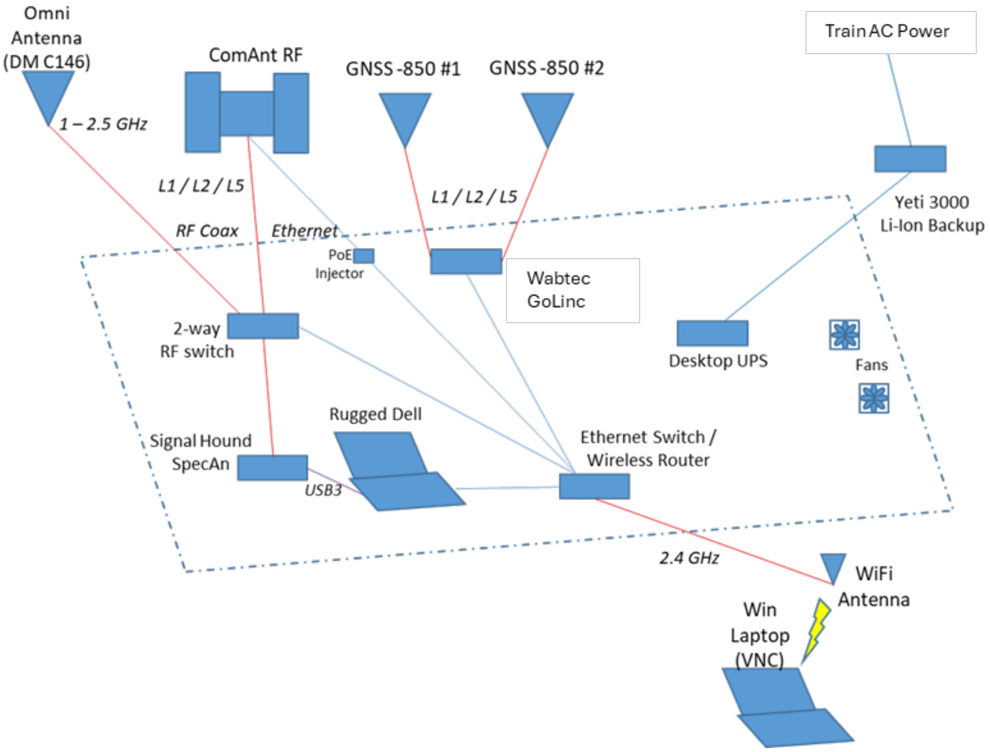


Figure 38: Survey System Schematic

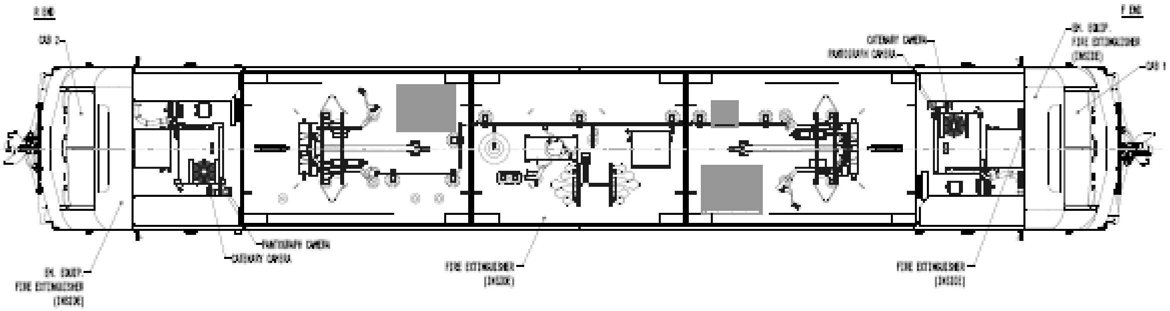


Figure 39: Line Diagram of ACS-64 Locomotive's roof[50]

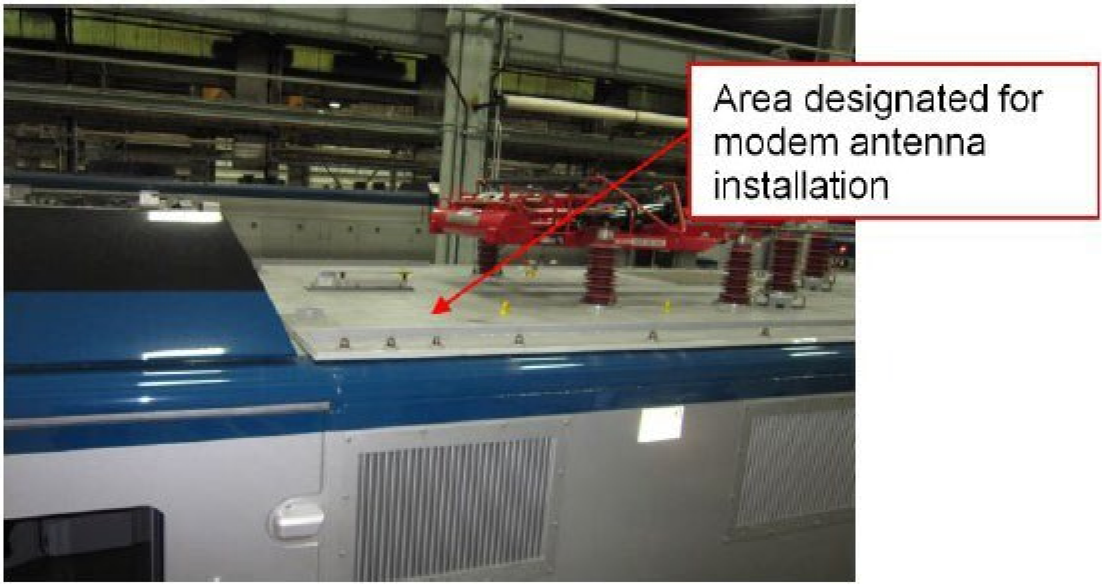


Figure 40: Locomotive roof detail showing installation location for 5G cellular antenna[51]

Precision Timing

The Frank LoBiondo Coast Guard Authorization Act of 2018 (Public Law 115–282) included Section 514, “Backup National Timing System,” also known as the National Timing Resilience and Security Act of 2018 (NTRSA).[52] The NTRSA required that, “Subject to the availability of appropriations, the Secretary of Transportation shall provide for the establishment, sustainment, and operation of a land-based, resilient, and reliable alternative timing system.” The goals of this measure were to reduce critical dependency on GPS, to provide a complement to GPS, and to ensure availability of uncorrupted and non-degraded timing signals.

The criticality of precision timekeeping for passenger rail extends to PTC as well as communications and scheduling. Amtrak, through discussions with the Volpe team, shared that interruptions in Timing signals contribute more strongly to service delays than disruptions of Position or Navigation. Examples include Amtrak’s underground stations in Chicago and covered stations at Milwaukee, where service typically suffers as much as 30 minutes of delay per train. Precision timing interruptions force Amtrak trains to rely on the internal clocks of their on-board Precision Navigation Modules. (The PNMs fall back to their internal clocks when they lose the GPS signal for timing. NTP servers are in work but not yet implemented.) All clocks, regardless of accuracy, are prone to drift and error over time; PNMs are no exception. Therefore, loss of GNSS signals results in loss of precision timekeeping for PTC aboard Amtrak trains in service.

Approaches to precision timing testing would leverage the Volpe Center’s prior work in this area. In 2019-2020, Volpe undertook a Complementary PNT and GPS Backup Technologies Demonstration.[53] Timing applications for rail will assess four attributes:

1. Coverage, i.e. service availability and uniformity across an appropriate area;
2. Accuracy and stability across an appropriate area;
3. Long-term accuracy and stability of time transfer to a fixed location; and
4. Time transfer availability and accuracy to a fixed location under challenged GPS signal conditions.

Volpe assessment of rail timing challenges and solutions would utilize one or more of the following test scenarios.

1. 72-Hour Bench Static Timing: Supports characterization of a technology's time transfer error over an extended period of continuous transmission. Each candidate PNT solution would be required to provide a one-pulse-per-second (1-pps) output connection that could then be measured against the timing standard produced by the appropriate static timing reference system. All equipment would be placed indoors.
2. Static Outdoor Timing: Collects continuous 60-minute timing data at three separate predetermined points in the demonstration area to assess candidate equipment performance in relation to the aforementioned attributes.
3. Static Indoor Timing: Enables continuous 60-minute time transfer data collection. In this scenario, time transfer data for candidate equipment are collected at three surveyed indoor points to assess each system's signal availability and time transfer accuracy at a fixed location under challenged GPS signal conditions. The points used in this scenario would be five pre-surveyed static indoor points, identical to those used in the next scenario (Static Basement Timing).
4. Static Basement Timing: Collect time transfer data simultaneously from all candidate solutions over a 60-minute period at a single location indoors and below grade. This is a severely challenging signal environment for RF technologies due to very high signal attenuation and the potential to experience multipath conditions, and is representative of the underground station challenges experienced by Amtrak.
5. Dynamic Timing Scenario: Establish baseline performance for RF-based CPNT time transfer and/or time synchronization capability while in motion, including accuracy and short-term stability of the time transfer error at fixed points along the scenario route. Service coverage, availability, and uniformity will also be evaluated. The varied dynamic elements with short stops are intended to represent mobile timing use-cases, such as ground transportation.

Respond and Recover

Phase 2 of this effort will include plans for Amtrak trains to respond to and recover from GNSS events, and in turn inform FRA planning for the future of PTC. Planning with FRA will encompass:

- Rail and PTC equipment in use, including
  - Trains, tracks, related electronics,

    - GNSS-specific: Hardware (antennas, receivers), Algorithms (fusion algorithms), Resiliency (self-nulling antennas), and
    - Non-GNSS e.g. inertial, odometry;
- Challenges faced: Disruptions, anomalies, others;
- Rail modeling, simulation, and test capabilities;
- A Workshop with Stakeholders for further planning and discussion, including
    - U.S. Government (DOT, OST, FRA),
    - Amtrak,
    - Assocation of American Railroads, and
    - Rail freight operators; and finally,
- Non-PNT areas of interest, such as RF communications.

Appendix A: Positive Train Control

PTC is the primary PNT dependency for rail. PTC is a GPS-based system designed to prevent train-to-train collisions, over-speed derailments, incursions into established work zone limits, and the movement of a train through a switch left in the wrong position. PTC is required on tracks with regularly scheduled intercity or commuter passenger rail service, and freight railroad main lines carrying hazardous materials.

PTC utilizes a combination of GPS and train-based sensors to determine a train's location relative to an on-board track database. [54] PNT data are fused in the on-board PTC architecture depicted in Figure 41 to provide a train's speed and position. Table 7 lists specifics on typical PNT data sources for PTC.

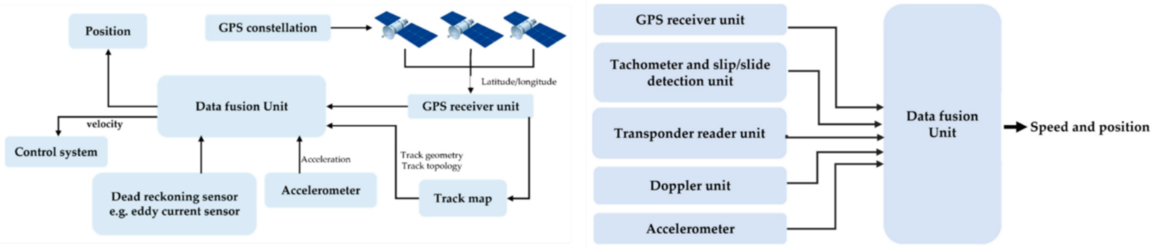


Figure 41: Current Rail Positioning Architecture [55]

Table 7: Characteristics of Current Train Positioning Sensors

Type	Sensor	Sensing Rate	Absolute Position	Relative Position	Outage Issue	Enviro. Impact
On-board	IMU	100 Hz	No	Yes	No	No
On-board	Wheel tachometer, odometer	10 Hz	No	Yes	No	Yes
On-board	GNSS	20 Hz	Yes	No	Yes	Yes
Track-side	RFID	N/A	No	Yes	No	Yes
Track-side	Balise	N/A	No	Yes	No	Yes

In a nominal PTC setup, an in-cab display utilizes the fused PNT data to provide track mapping through the onboard database while also informing the operator of track speed limits, grade, elevation, switches, signals, work zones, train speed, changes in elevation, and train authority. In turn, the onboard computer displays upcoming speed and braking changes, and the onboard PTC computer will automatically slow and/or stop a train where needed if the engineer does not do so. In this way, trains rely on PNT to locate themselves relative to their on-board track databases. Figure 42, Figure 43, and Figure 44 depict examples of this setup.

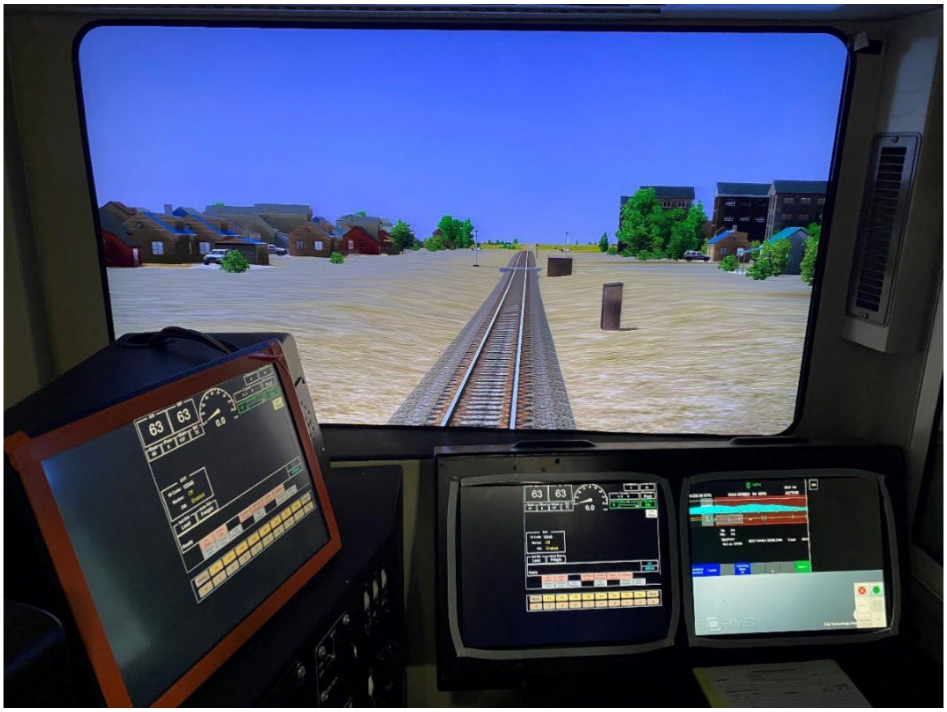
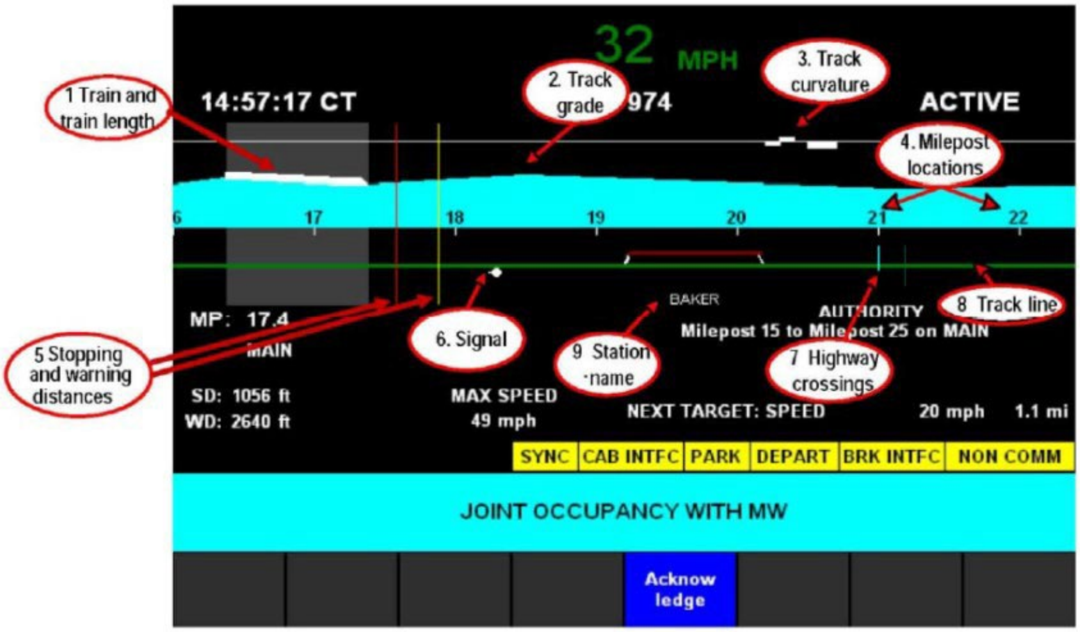


Figure 42: Freight Train Operator displays with PTC display at bottom-right[56]



32 MPH

14:57:17 CT

974

ACTIVE

MP: 17.4
MAIN

SD: 1056 ft
WD: 2640 ft

MAX SPEED
49 mph

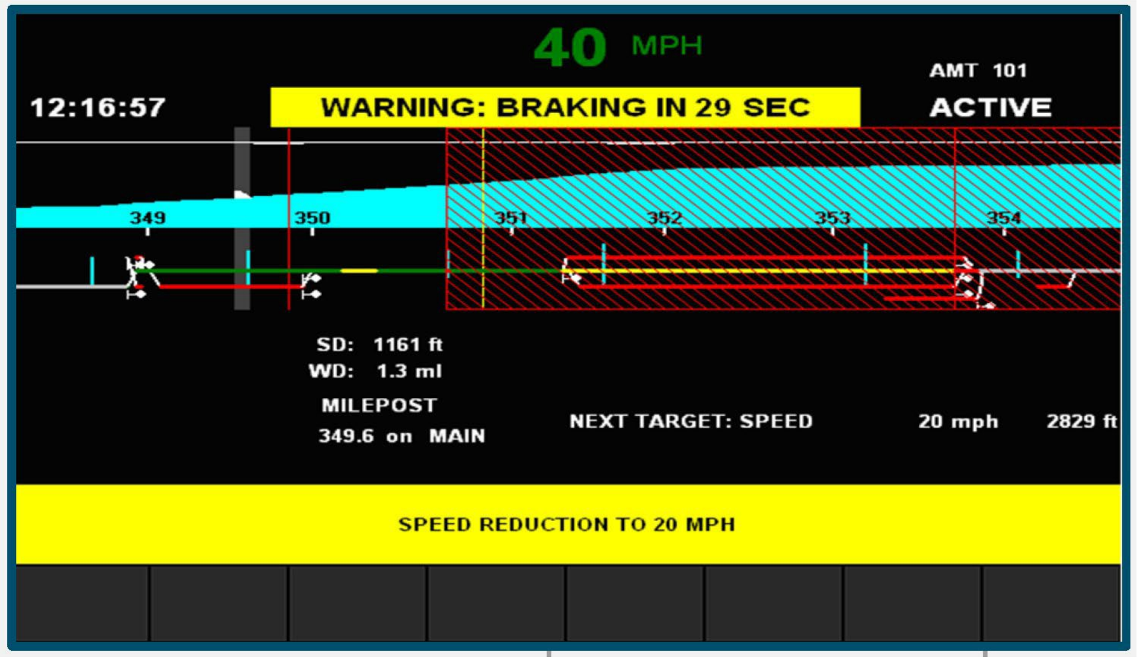
BAKER

AUTHORITY
Milepost 15 to Milepost 25 on MAIN

NEXT TARGET: SPEED 20 mph 1.1 mi

JOINT OCCUPANCY WITH MW

Figure 43: PTC Display indicating Open Rail ahead [57]



40 MPH

12:16:57

WARNING: BRAKING IN 29 SEC

AMT 101

ACTIVE

SD: 1161 ft
WD: 1.3 mi

MILEPOST
349.6 on MAIN

NEXT TARGET: SPEED 20 mph 2829 ft

SPEED REDUCTION TO 20 MPH

Figure 44: PTC Display indicating Speed Restriction ahead[58]

The most fundamental PTC type is the Incremental Train Control System (ITCS). Data from rail operator RF networks furnish the primary data source for the operator's PTC display.[59]

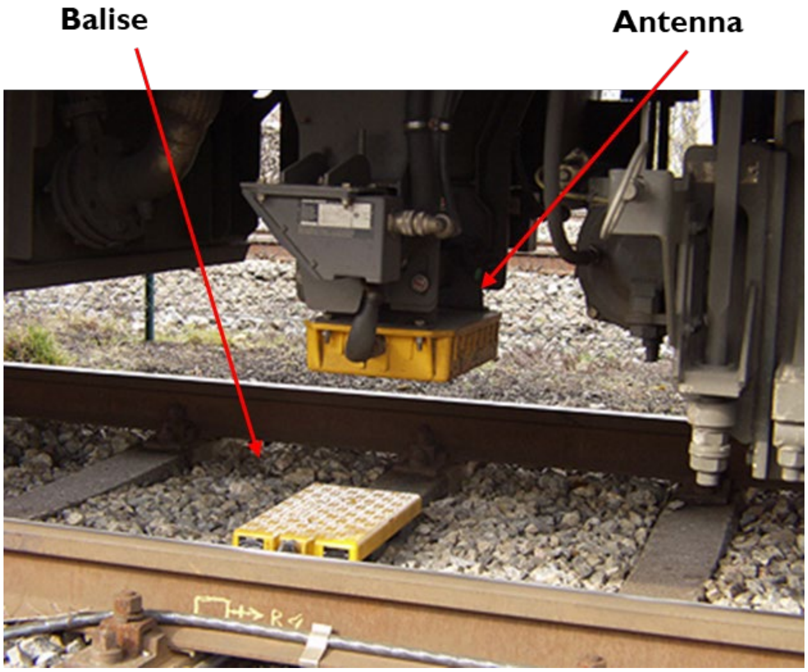


Figure 45: Typical Balise installation

Local commuter systems typically implement the Enhanced Automatic Train Control (E-ATC) system for PTC. E-ATC builds upon ITCS and meets the full FRA requirements of PTC by providing cab signal systems, centralized traffic control systems, and other operator signals or train control system enhancements. (Los Angeles' CALTRAIN network uses a similar system, Interoperable Incremental Train Control System (I-ITCS), which adds GPS-based train positioning and supports train speeds up to 110 MPH.)

Amtrak passenger trains in the NEC utilize a combination of cab signals and ACSES II. The latter is a transponder-based train positioning system capable of supporting trains running up to 150 MPH, such as the Acela Express. Balises, or transponders, are commonly used worldwide for inter-city passenger rail, including high-speed rail.[60] The transponders in this type of system are mounted in the train tracks and transmit their individual geographic locations along with other information, such as rail line geometry and speed restrictions. They typically need no power source, responding to radio frequency energy broadcast from train-mounted antennas. These antennas, installed under the train, receive the messages from the balises and pass them to the train's on-board computer. The computer then monitors and if necessary, restricts train speed, per the PTC operation stated previously. Balises are deployed in pairs so that a train can distinguish the direction of travel along the track. A typical installation is depicted in Figure 45.

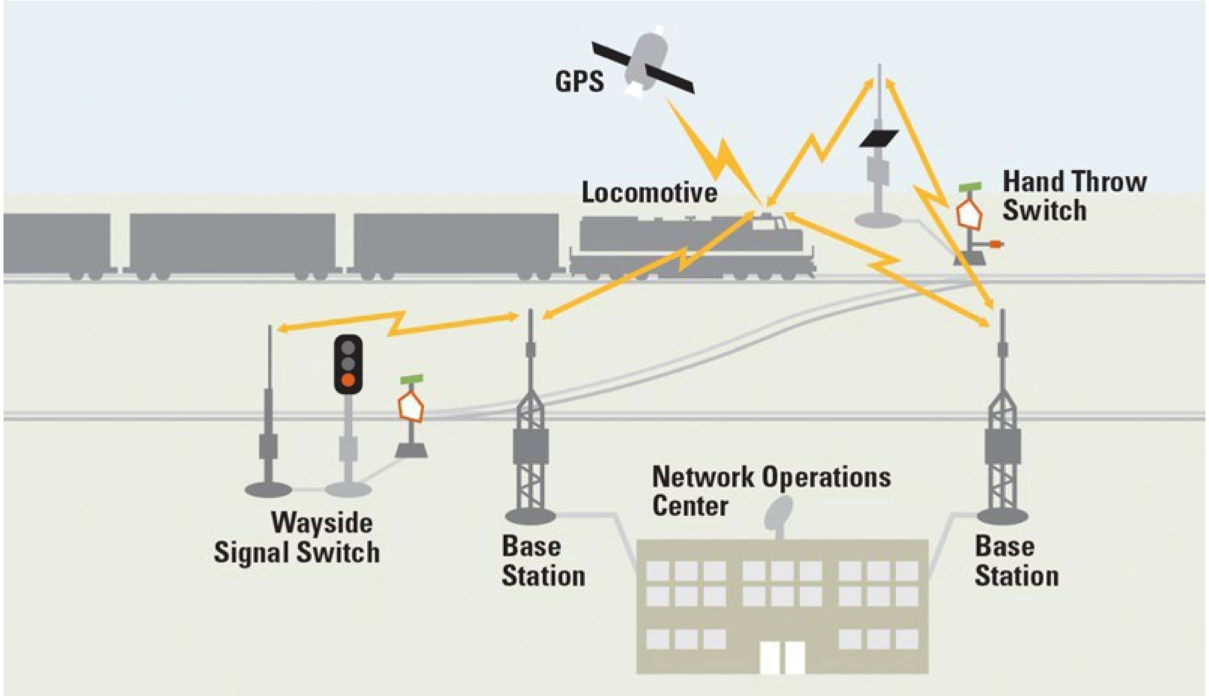


Figure 46: Schematic of I-ETMS system implementation of PTC[61]

Finally, major freight rail operators have implemented the Interoperable Electronic Train Management System (I-ETMS). I-ETMS utilizes a combination of GPS, on-board maps, and on-board sensors (including wheel tachometers and speed sensors) to determine a train's location within the on-board map. Trains utilize GPS to locate themselves on their on-board track database, with GPS providing data for an overlay of position information. Trains communicate their GPS-sourced position, velocity, and time over a dedicated RF communications network. This terrestrial RF network includes Wi-Fi, Cellular, and dedicated radio communication networks to connect trains, switches on tracks, and railroad dispatch offices. Data over the network includes track speed limits, grade, (changes in) elevation, switches, signals, and work zones; train speed; and train authority. For most Amtrak service outside of the NEC operating on rail equipped with I-ETMS, Amtrak trains must be interoperable with I-ETMS. Hence this is a focus for the pilot project. A schematic of the I-ETMS system is provided in Figure 46.

PTC inherently provides limited GNSS spoofing protection. Railroads utilize track maps and algorithms that detect and then protect when a signal deviates by 2.9 meters from the track map. If a train's PNT system shows a sudden large position shift, PTC would stop the train. Future PTC capabilities will include NTP servers, thus a sudden time shift would likewise bring a train to a stop.

Appendix B: NAVFEST Scenario Time Frames

This appendix contains plots comparing scheduled and observed scenario time frames for all nights of testing at NAVFEST.

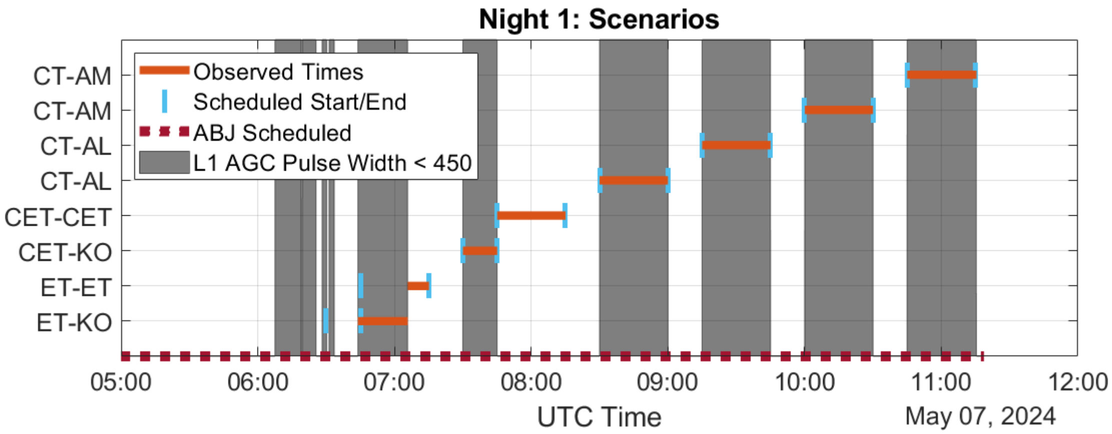


Figure 47. Scenario time frames for Night 1

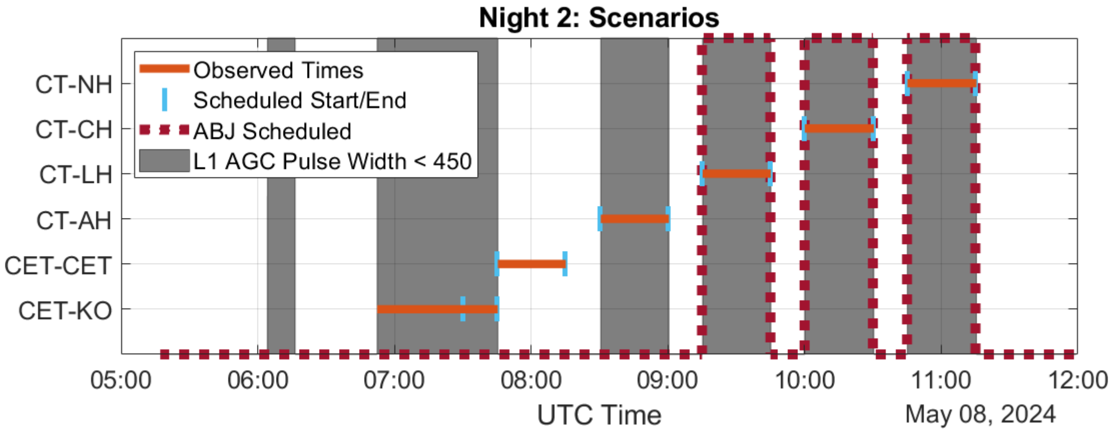


Figure 48. Scenario time frames for Night 2

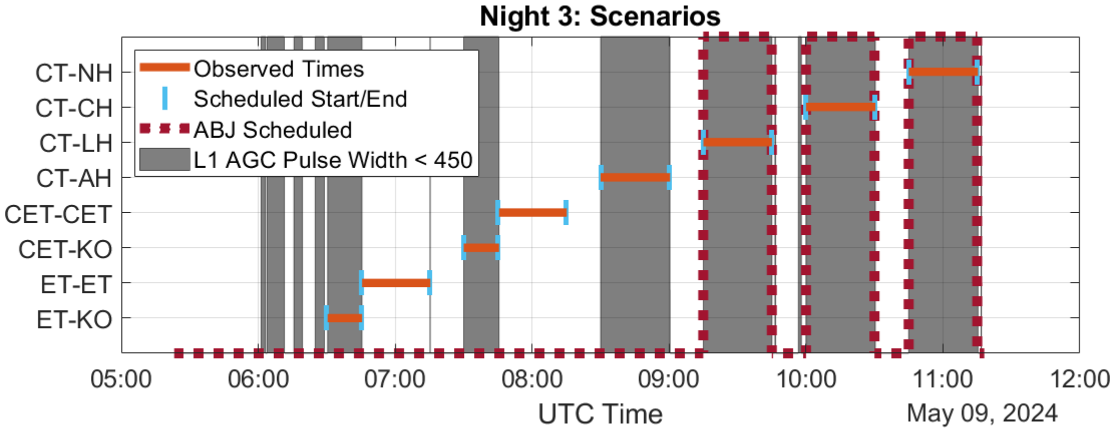


Figure 49. Scenario time frames for Night 3

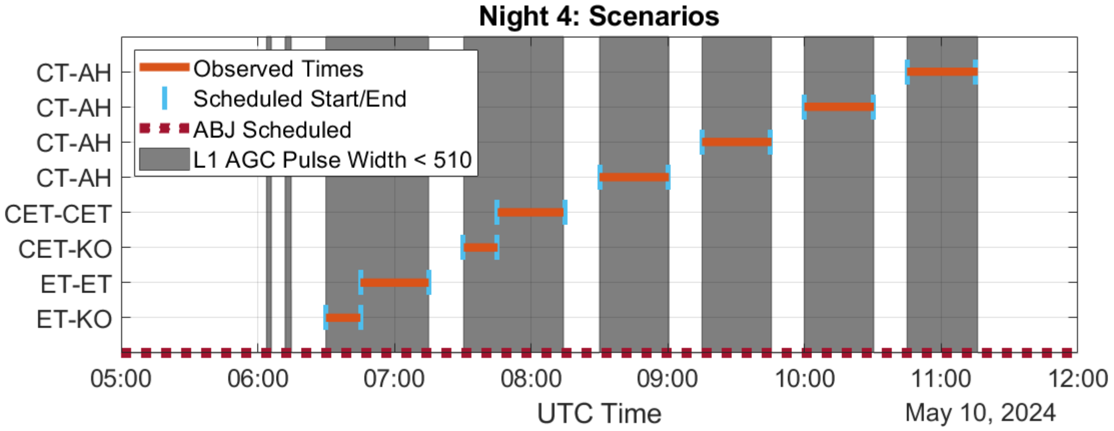


Figure 50. Scenario time frames for Night 4

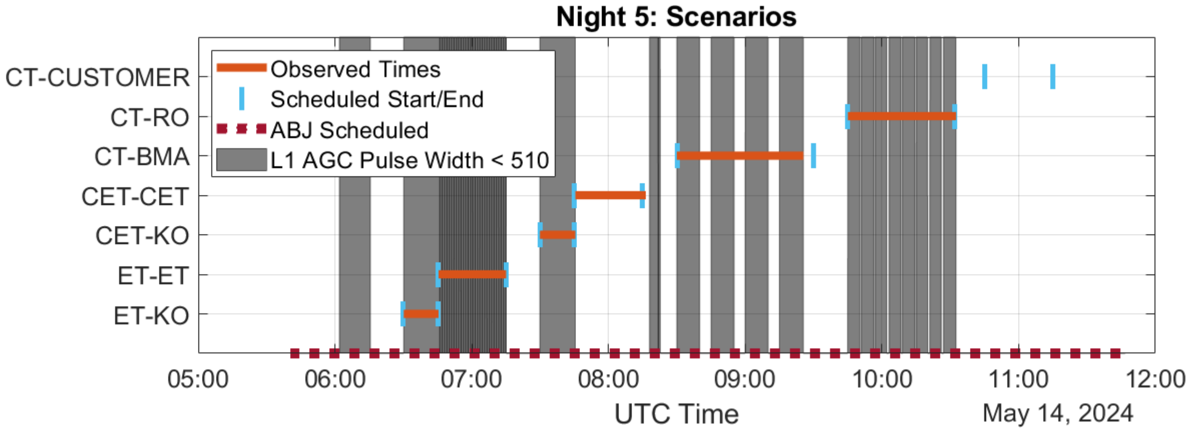


Figure 51. Scenario time frames for Night 5

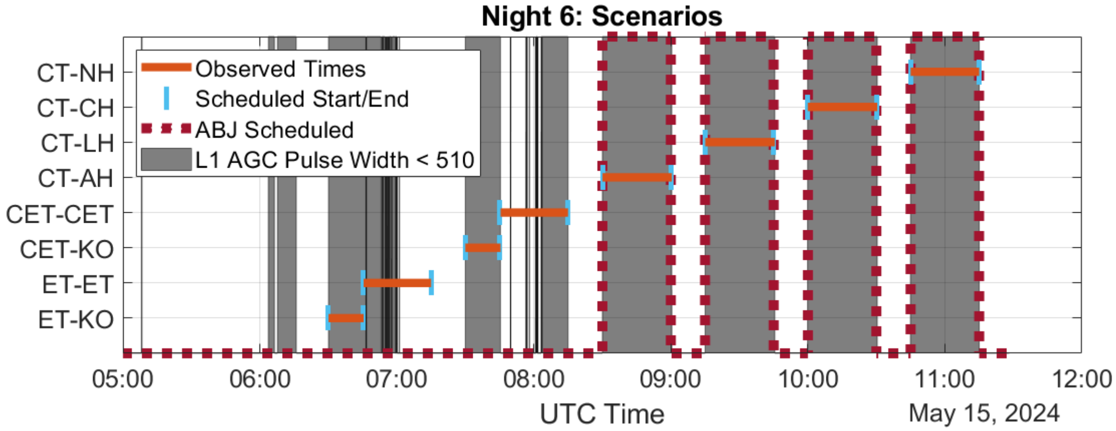


Figure 52. Scenario time frames for Night 6

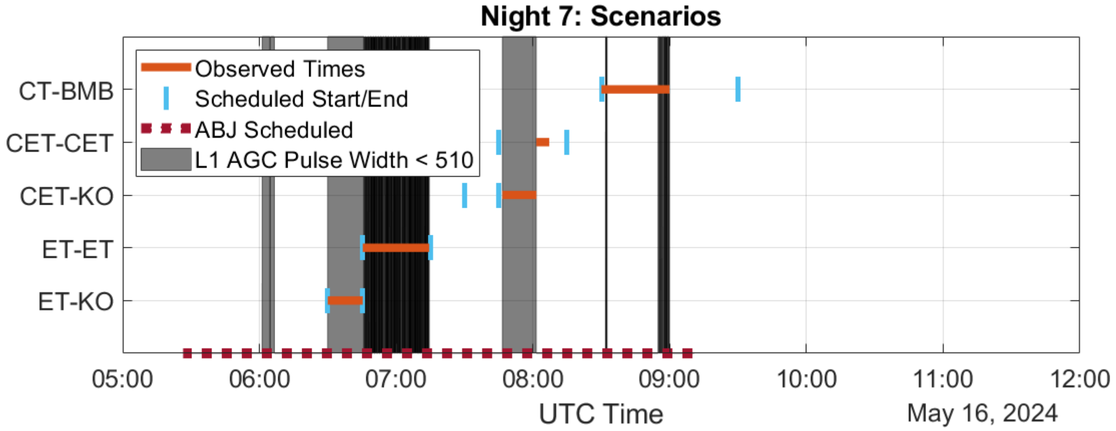


Figure 53. Scenario time frames for Night 7

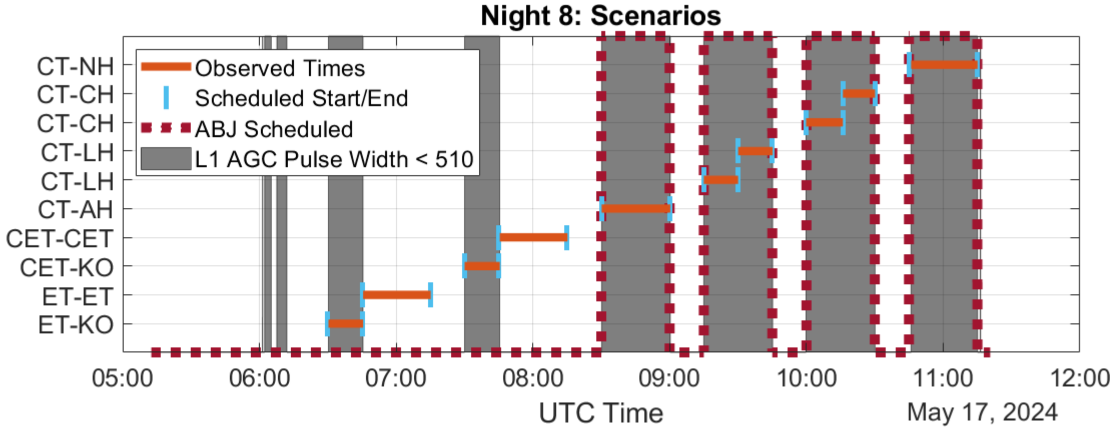


Figure 54. Scenario time frames for Night 8

Appendix C: NAVFEST Static Response Analysis Time Series Plots

This appendix contains horizontal position error time series plots for all scenarios used in the NAVFEST static response analysis.

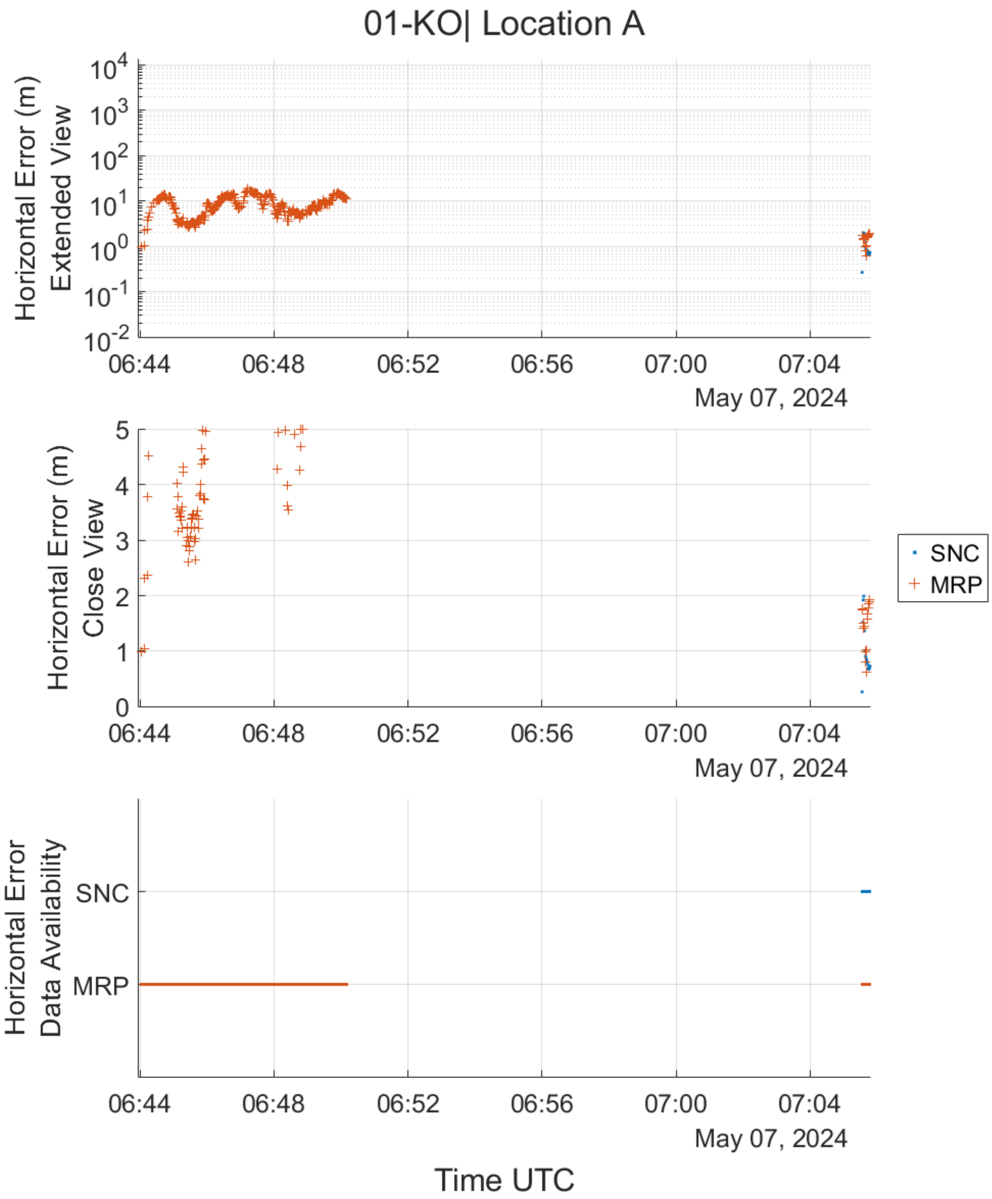


Figure 55. Horizontal position errors during scenario 01-KO

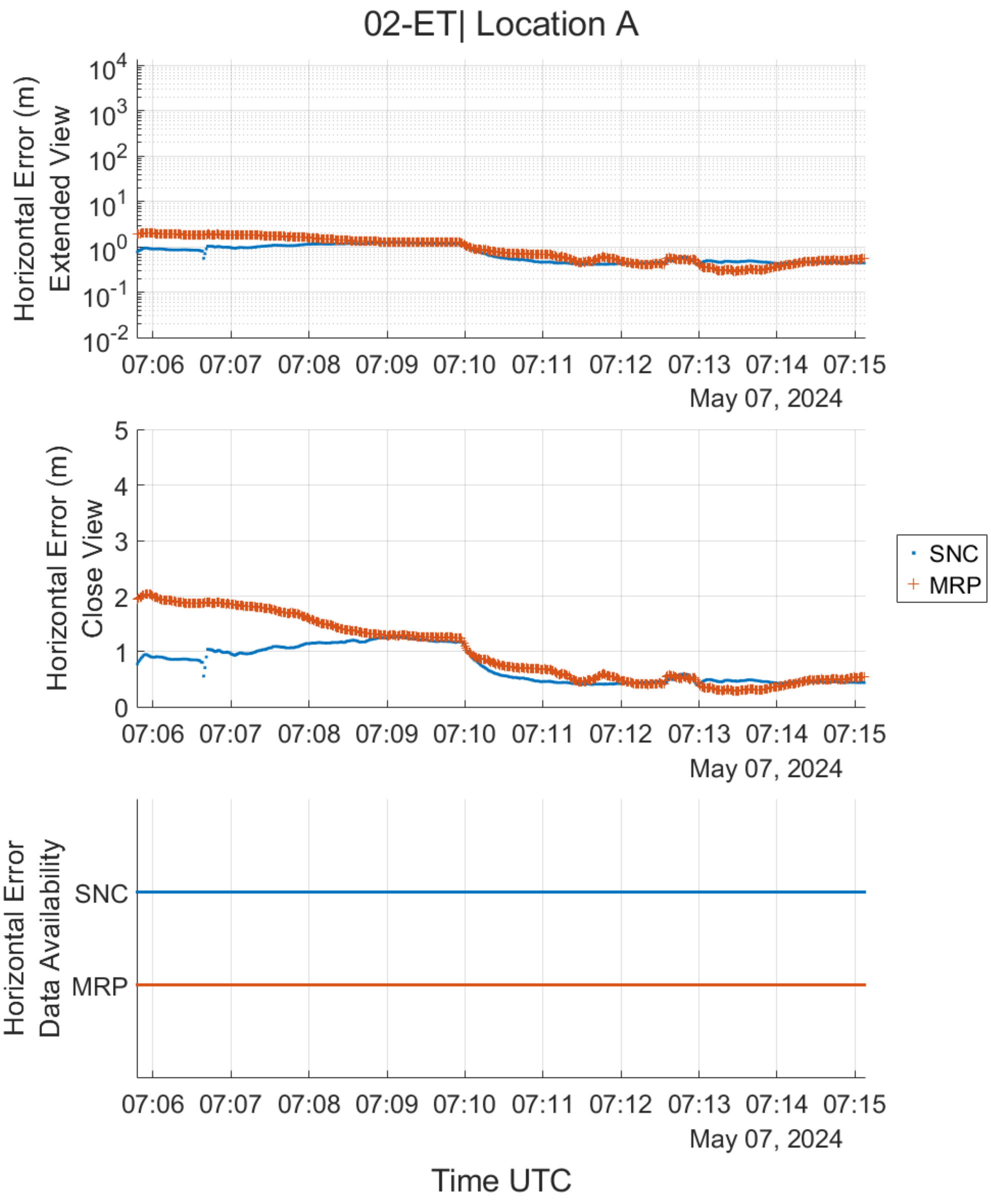


Figure 56. Horizontal position errors during scenario 02-ET

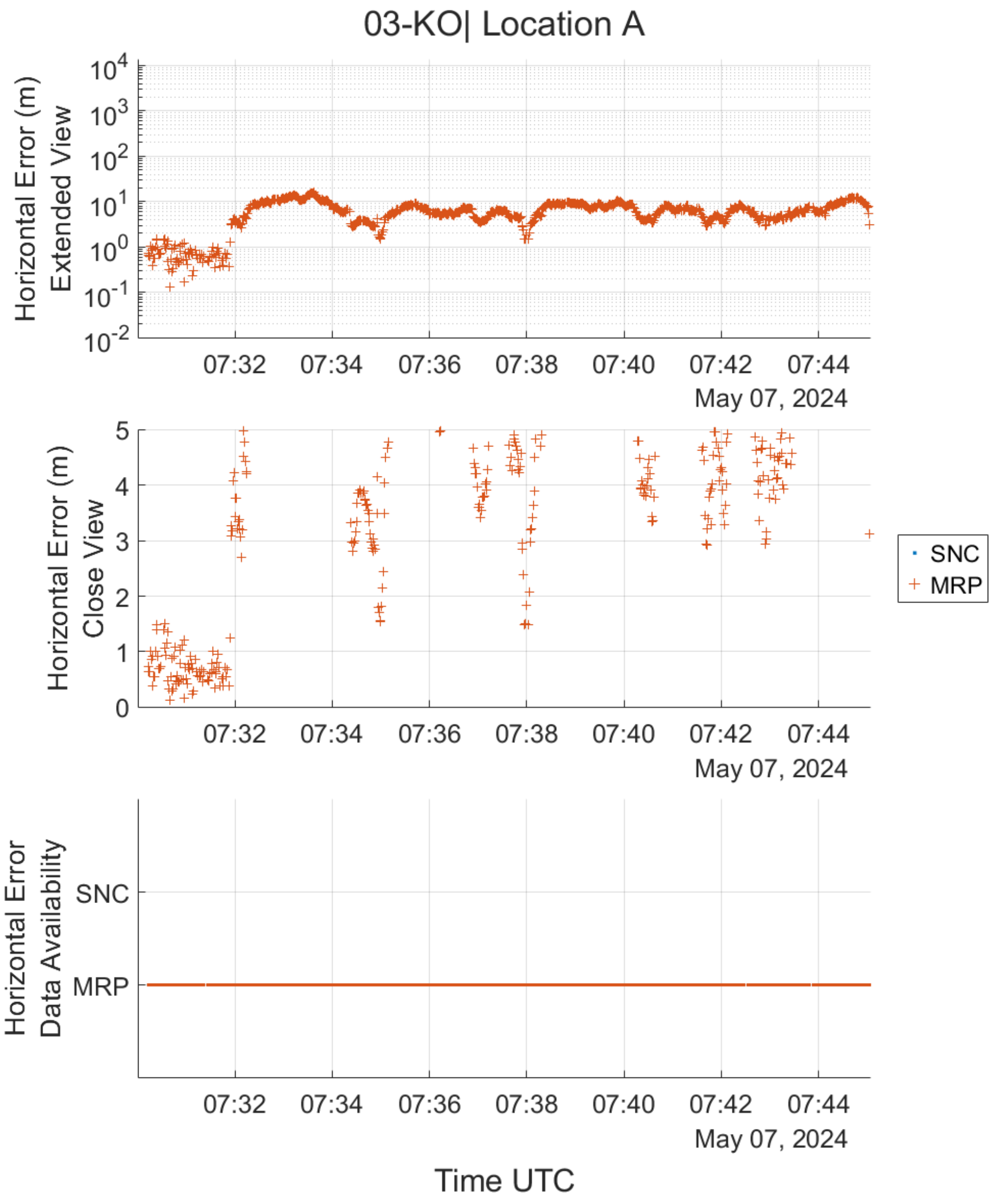


Figure 57. Horizontal position errors during scenario 03-KO

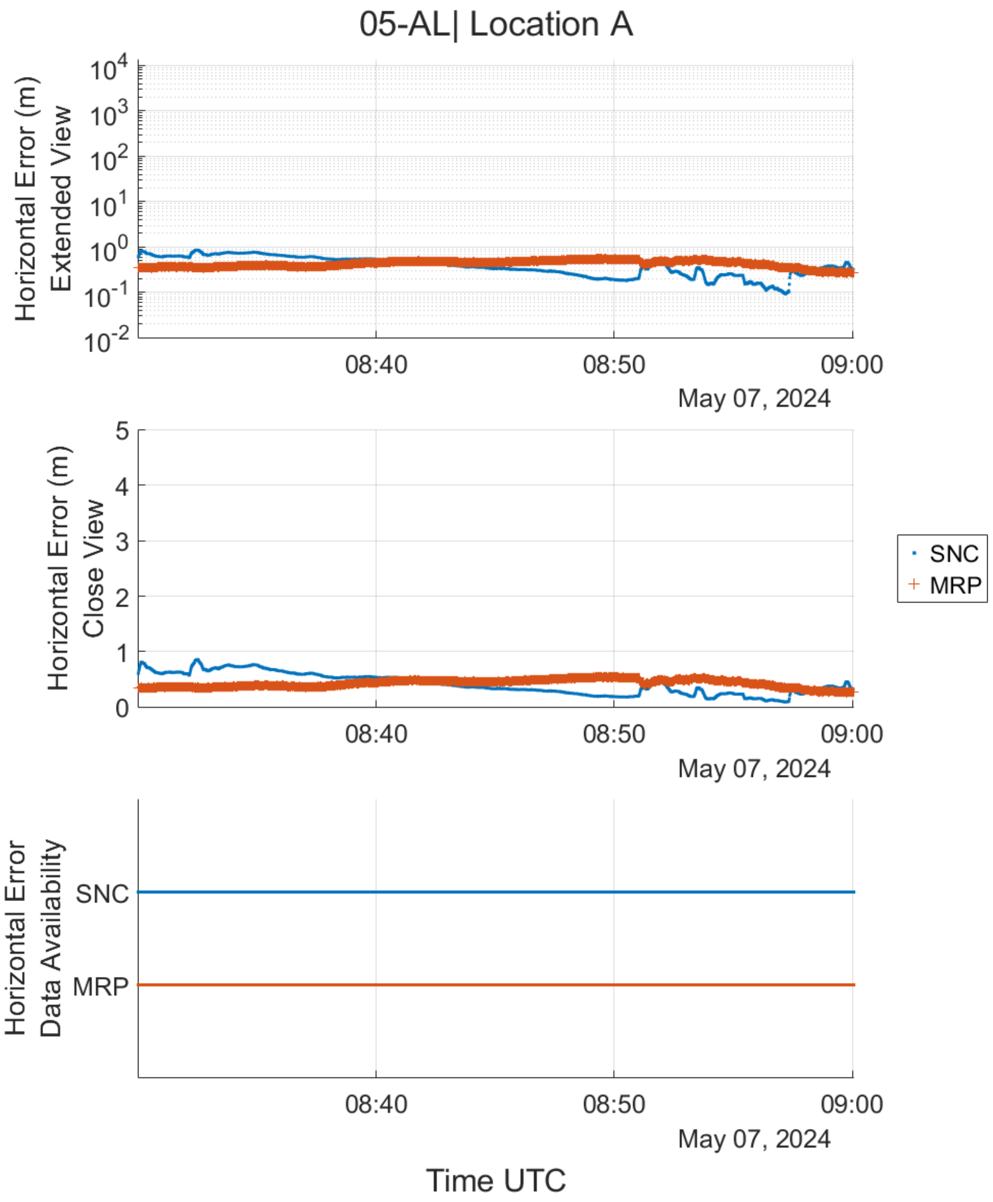


Figure 58. Horizontal position errors during scenario 05-AL

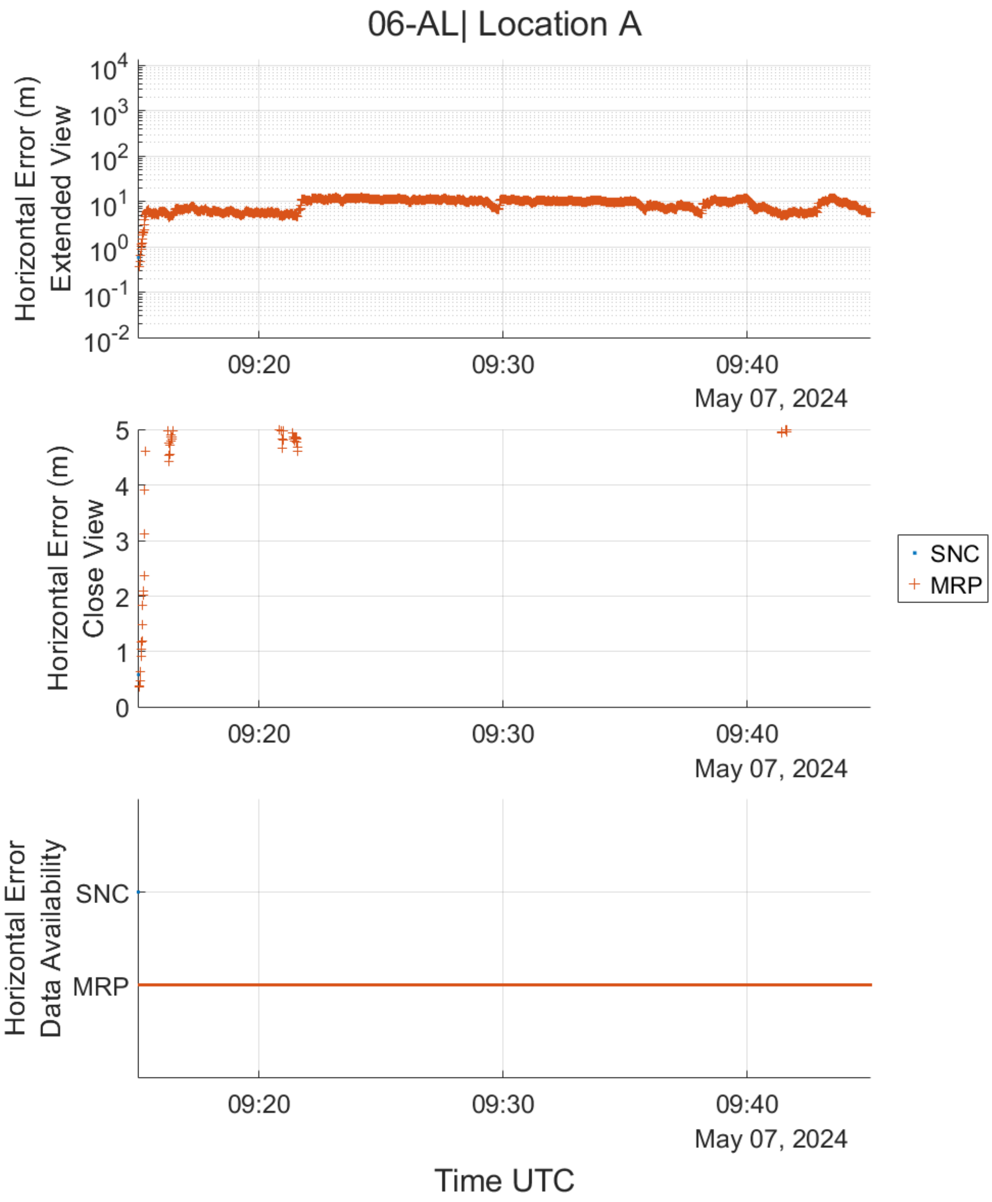


Figure 59. Horizontal position errors during scenario 06-AL

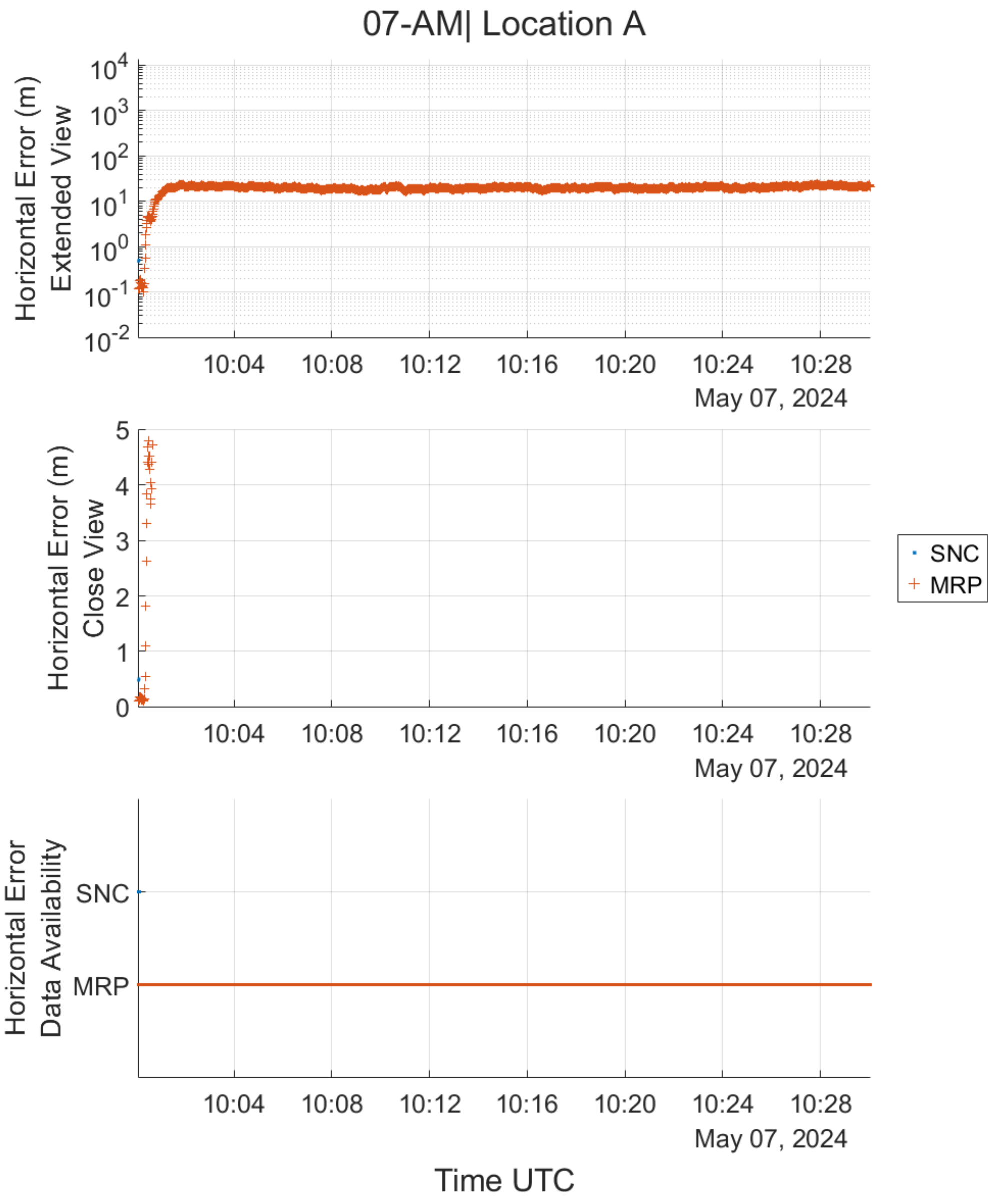


Figure 60. Horizontal position errors during scenario 07-AM

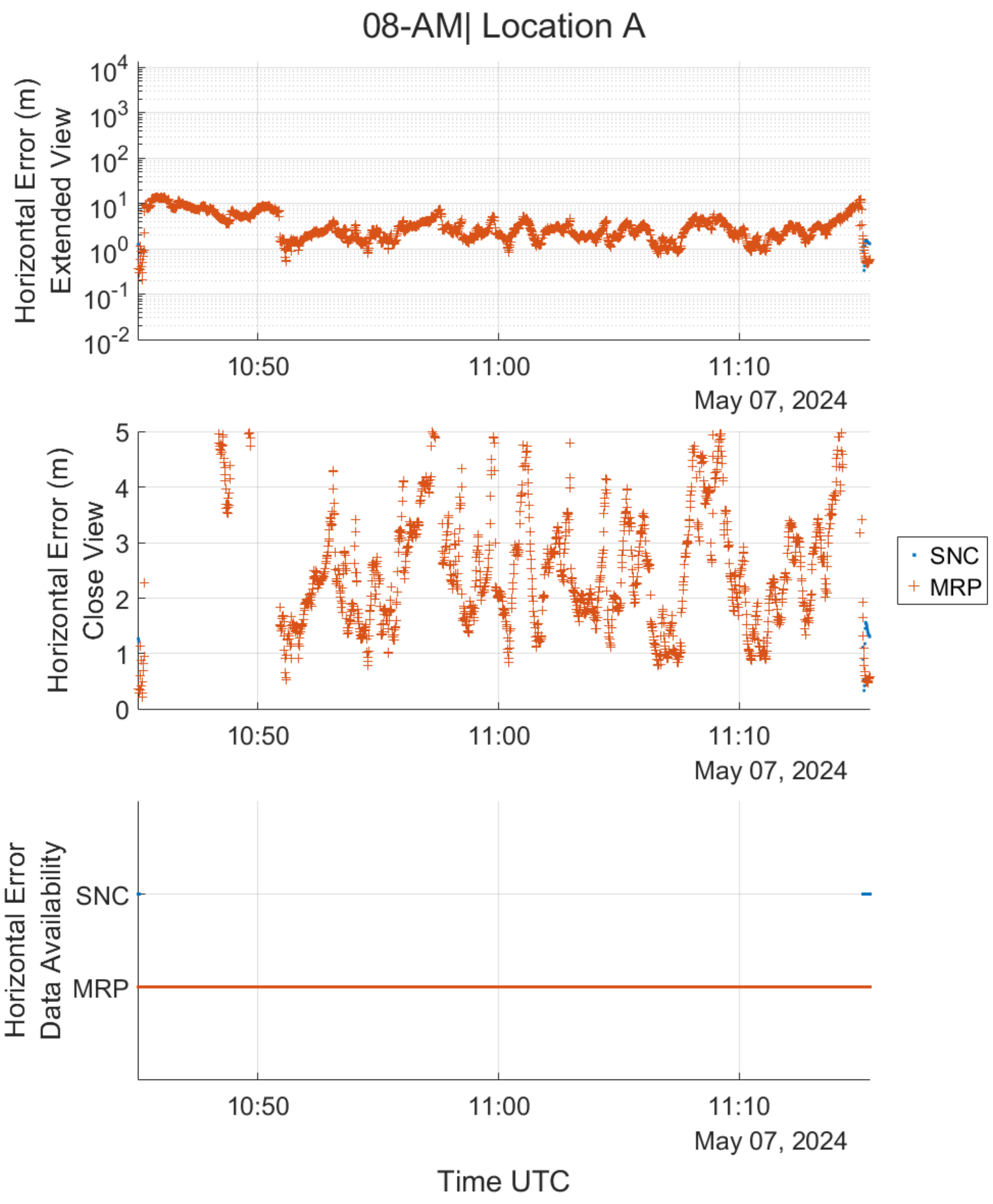


Figure 61. Horizontal position errors during scenario 08-AM

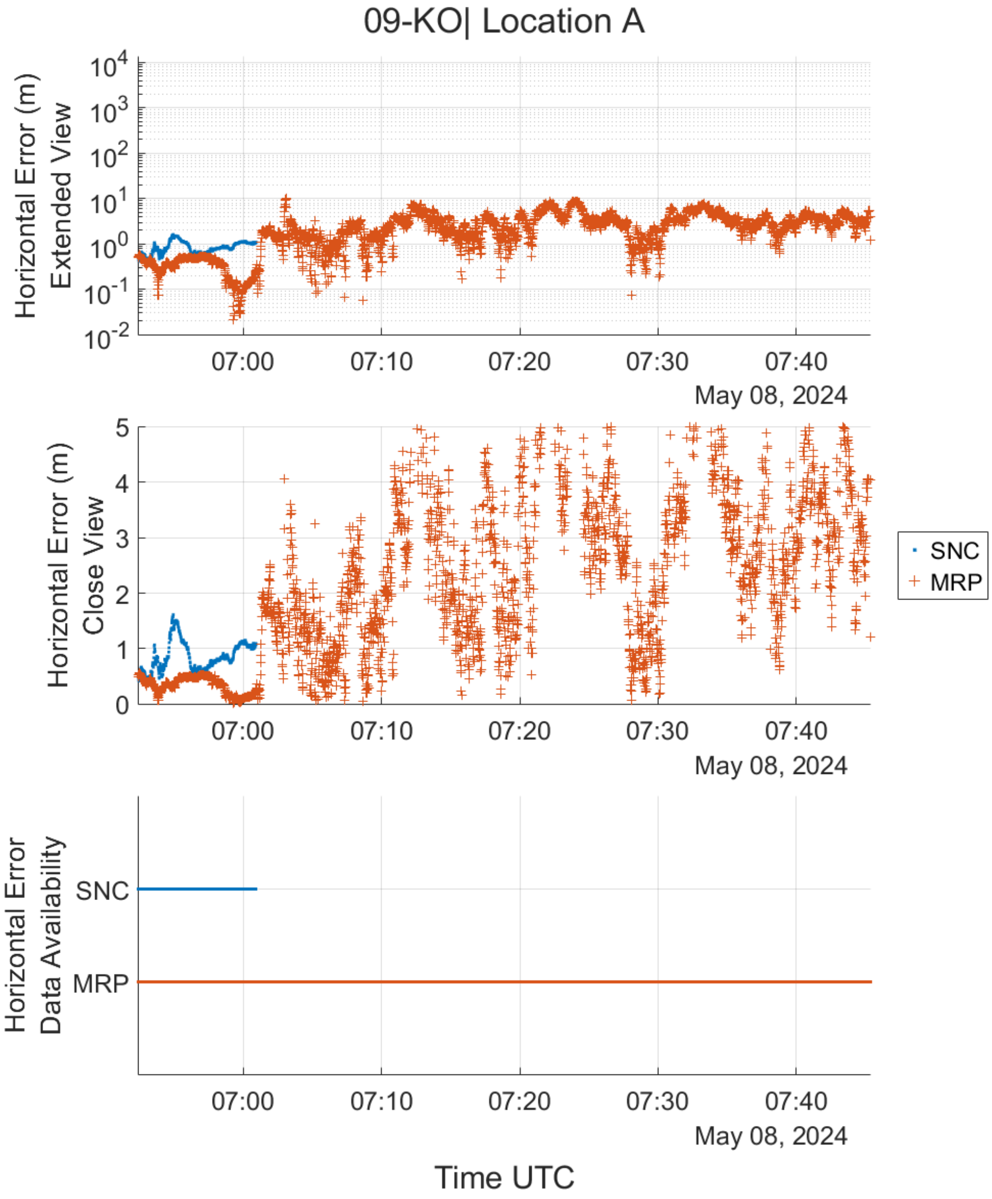


Figure 62. Horizontal position errors during scenario 09-KO

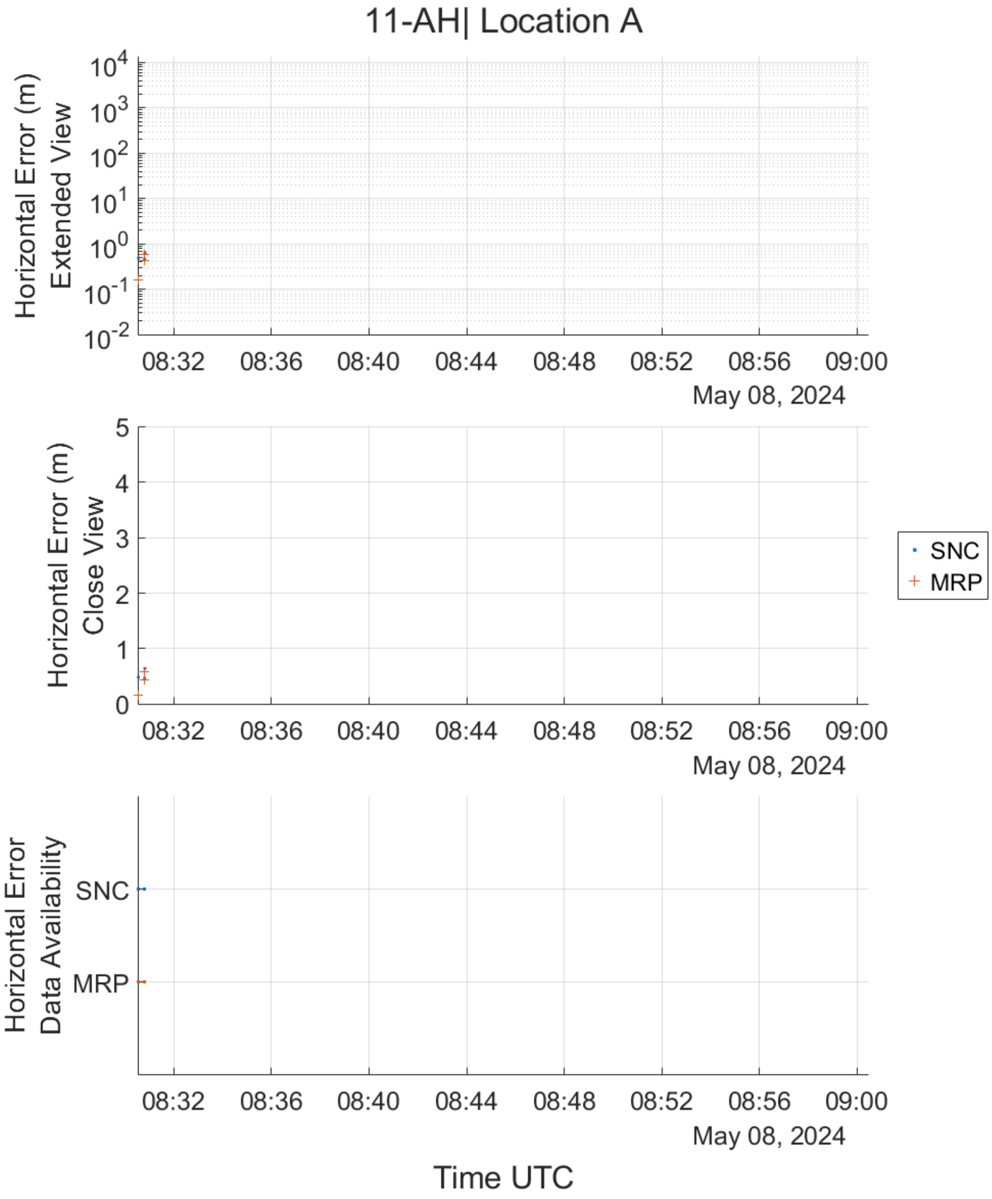


Figure 63. Horizontal position errors during scenario 11-AH

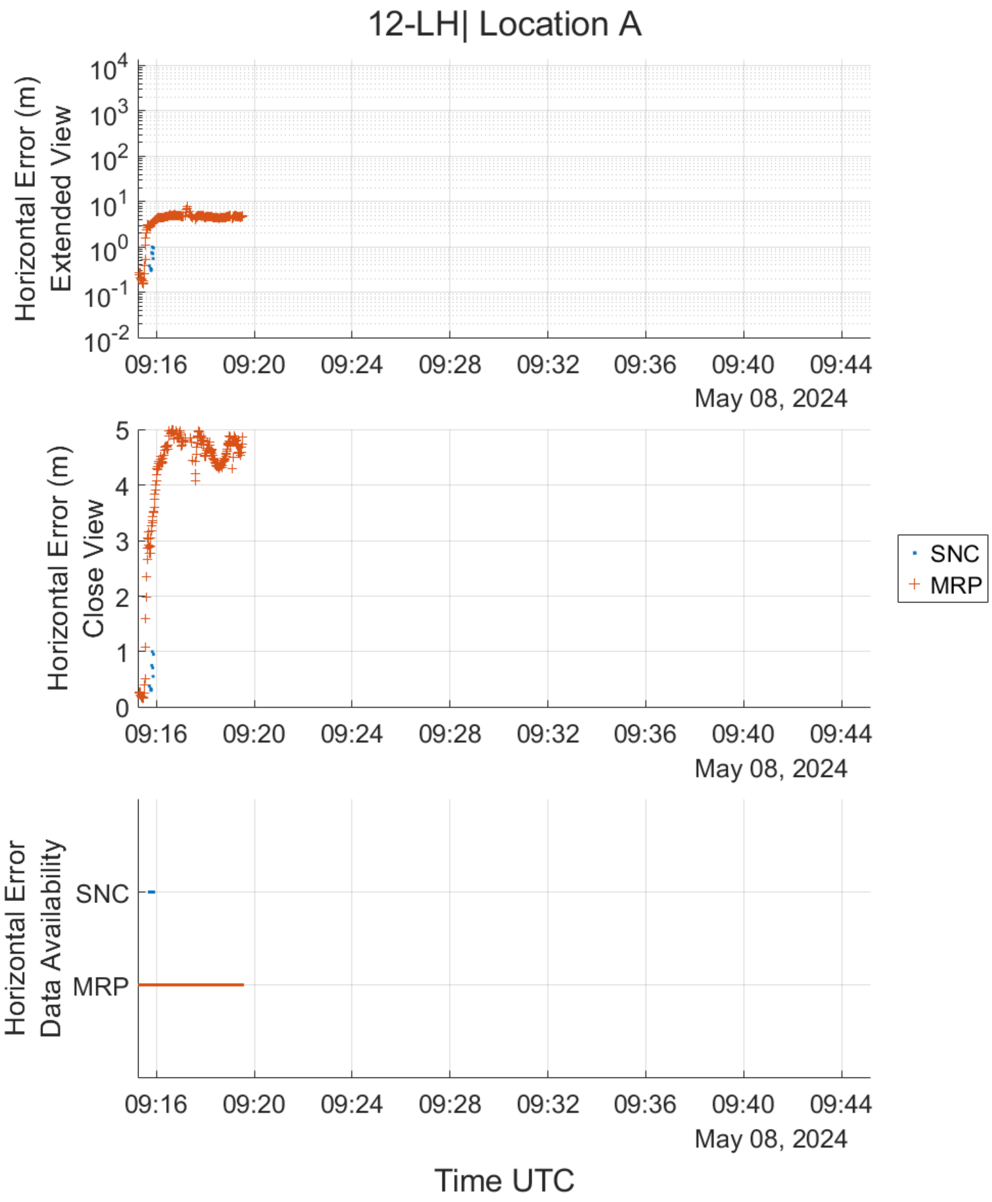


Figure 64. Horizontal position errors during scenario 12-LH

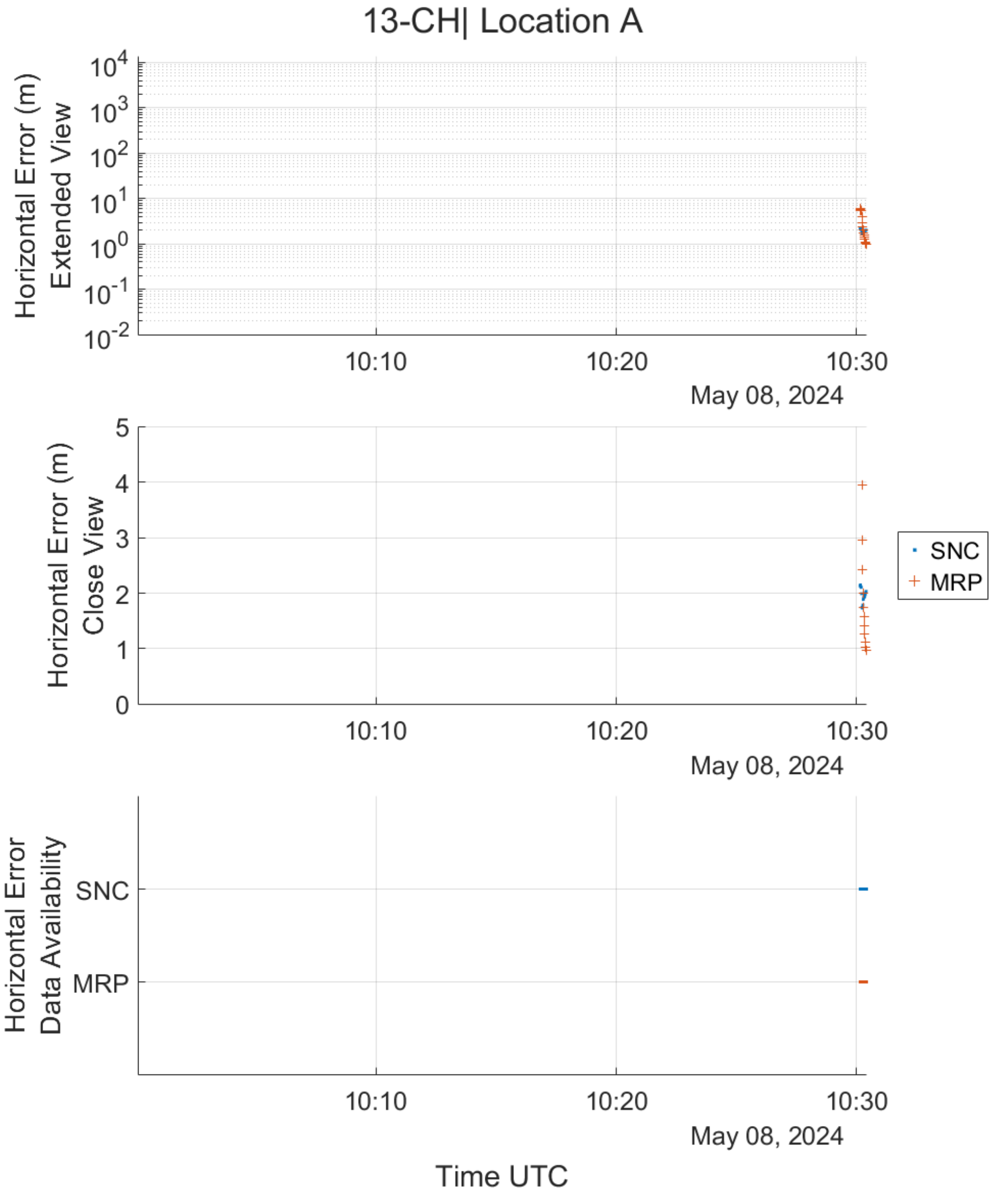


Figure 65. Horizontal position errors during scenario 13-CH

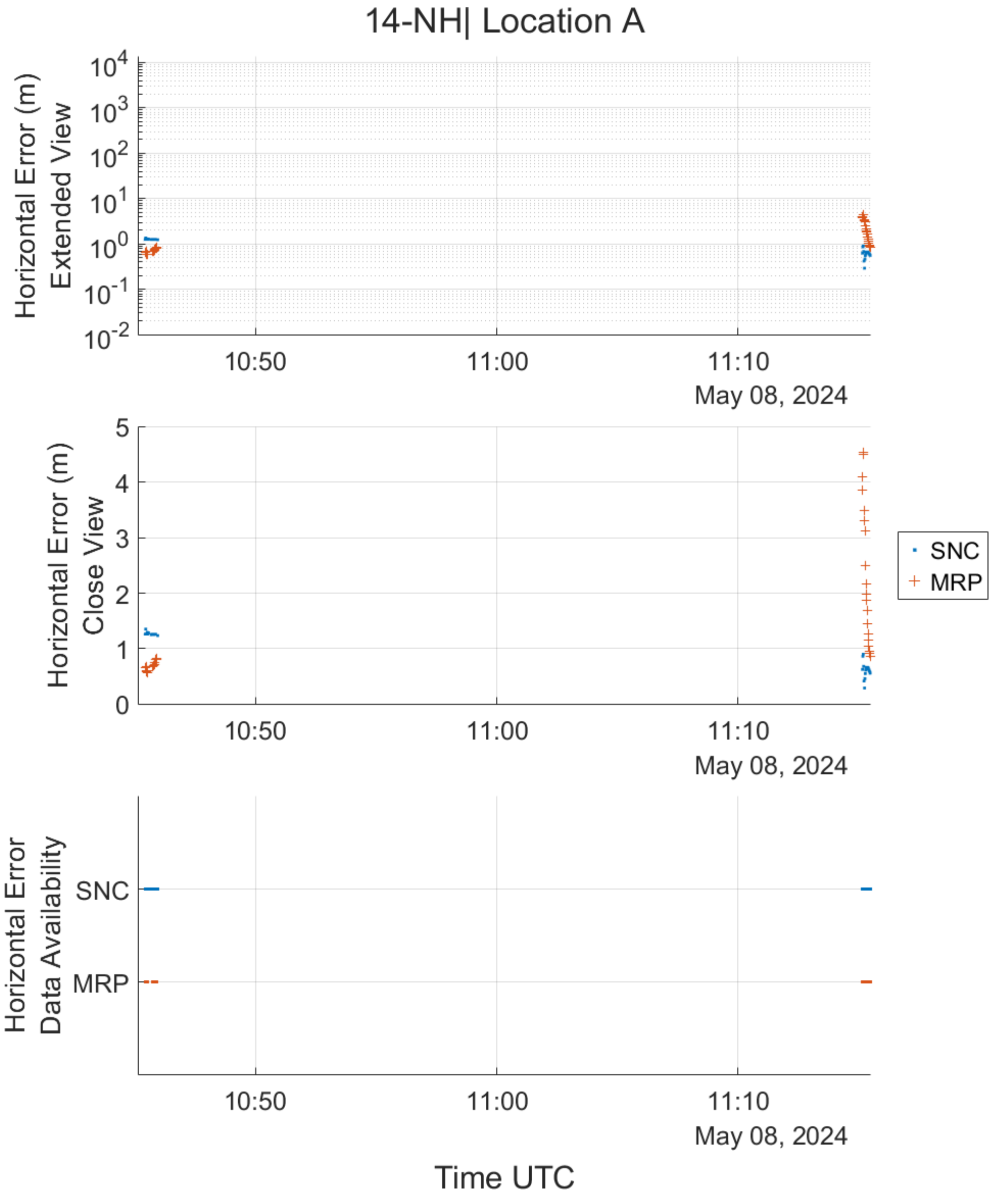


Figure 66. Horizontal position errors during scenario 14-NH

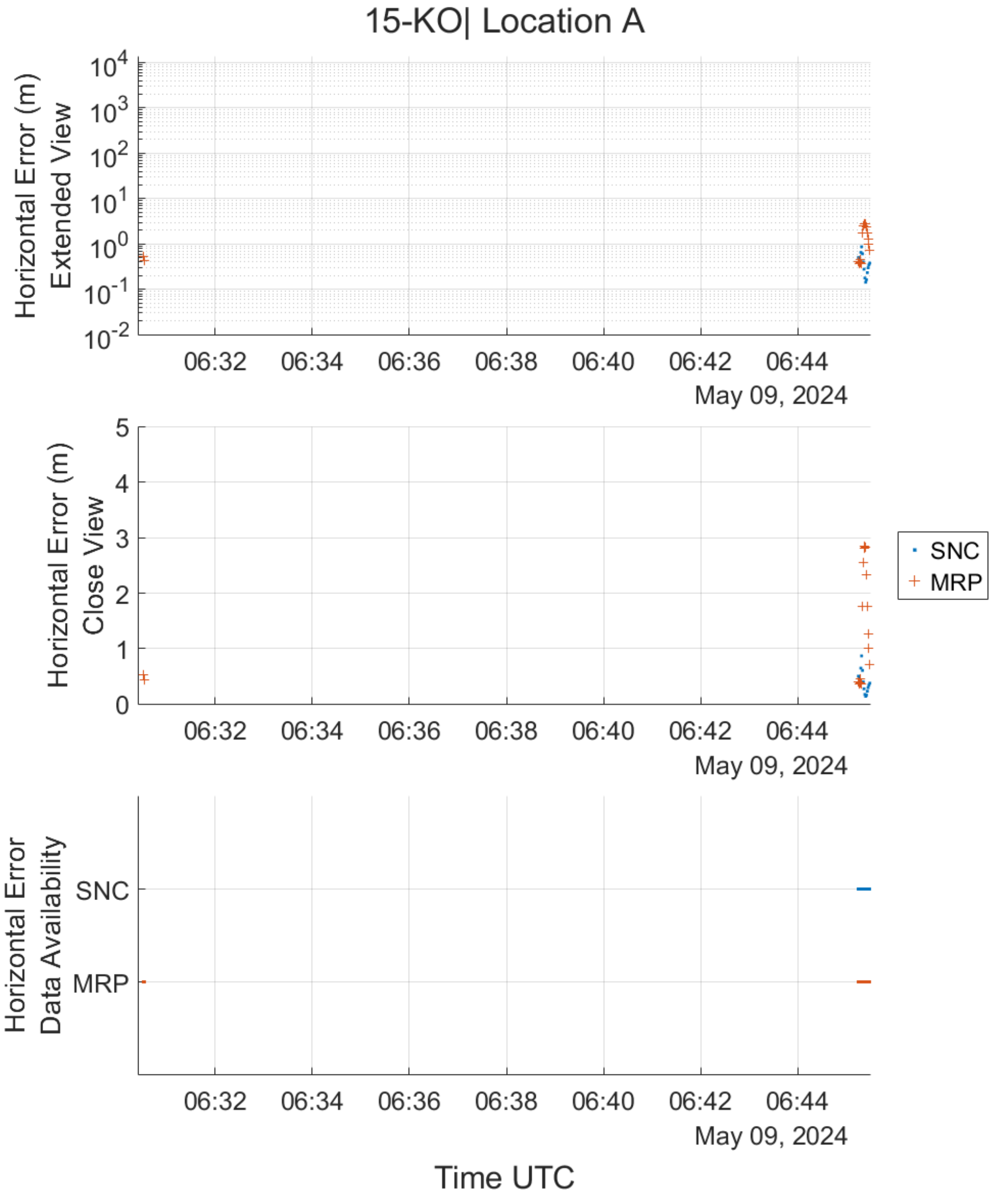


Figure 67. Horizontal position errors during scenario 15-KO

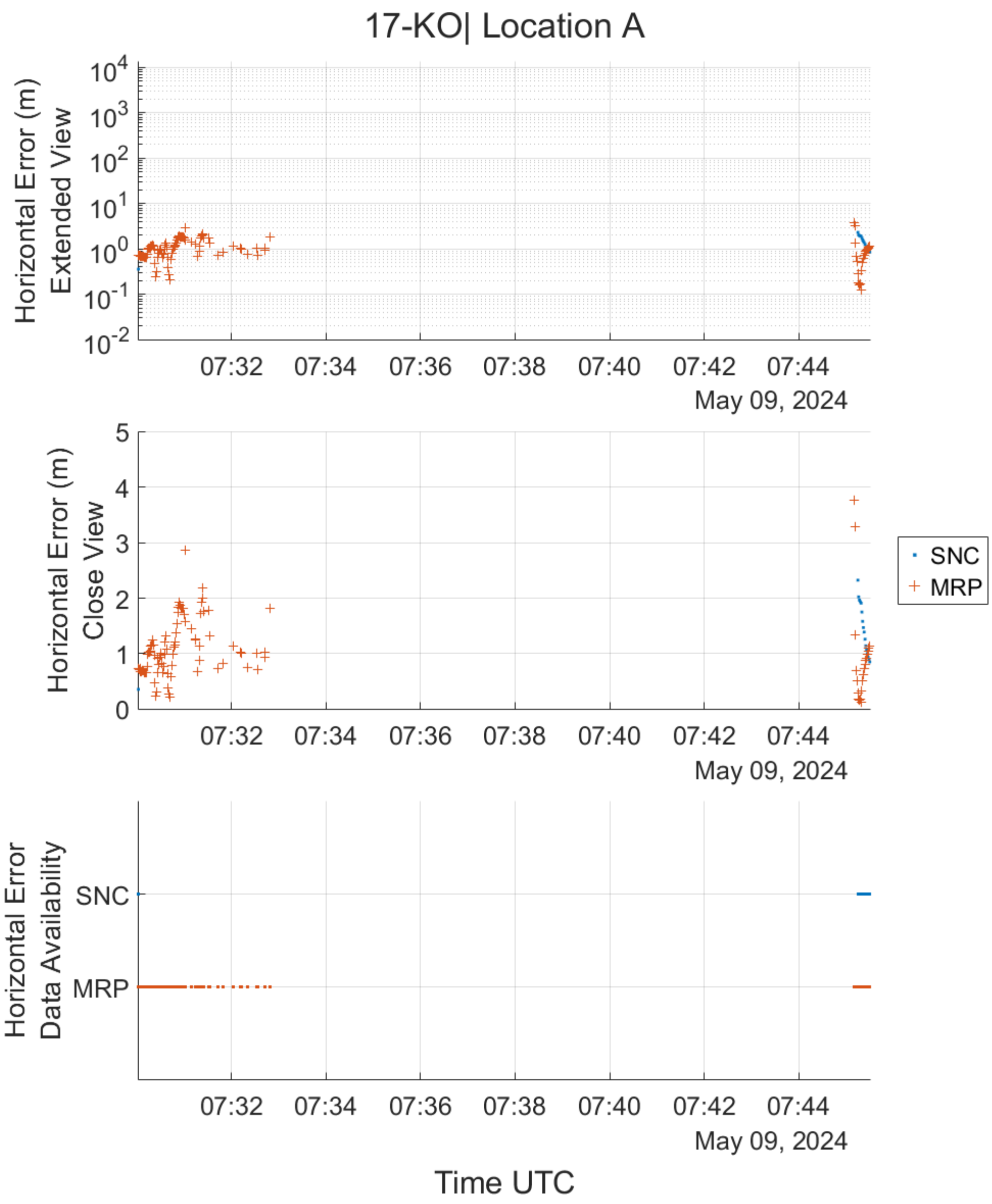


Figure 68. Horizontal position errors during scenario 17-KO

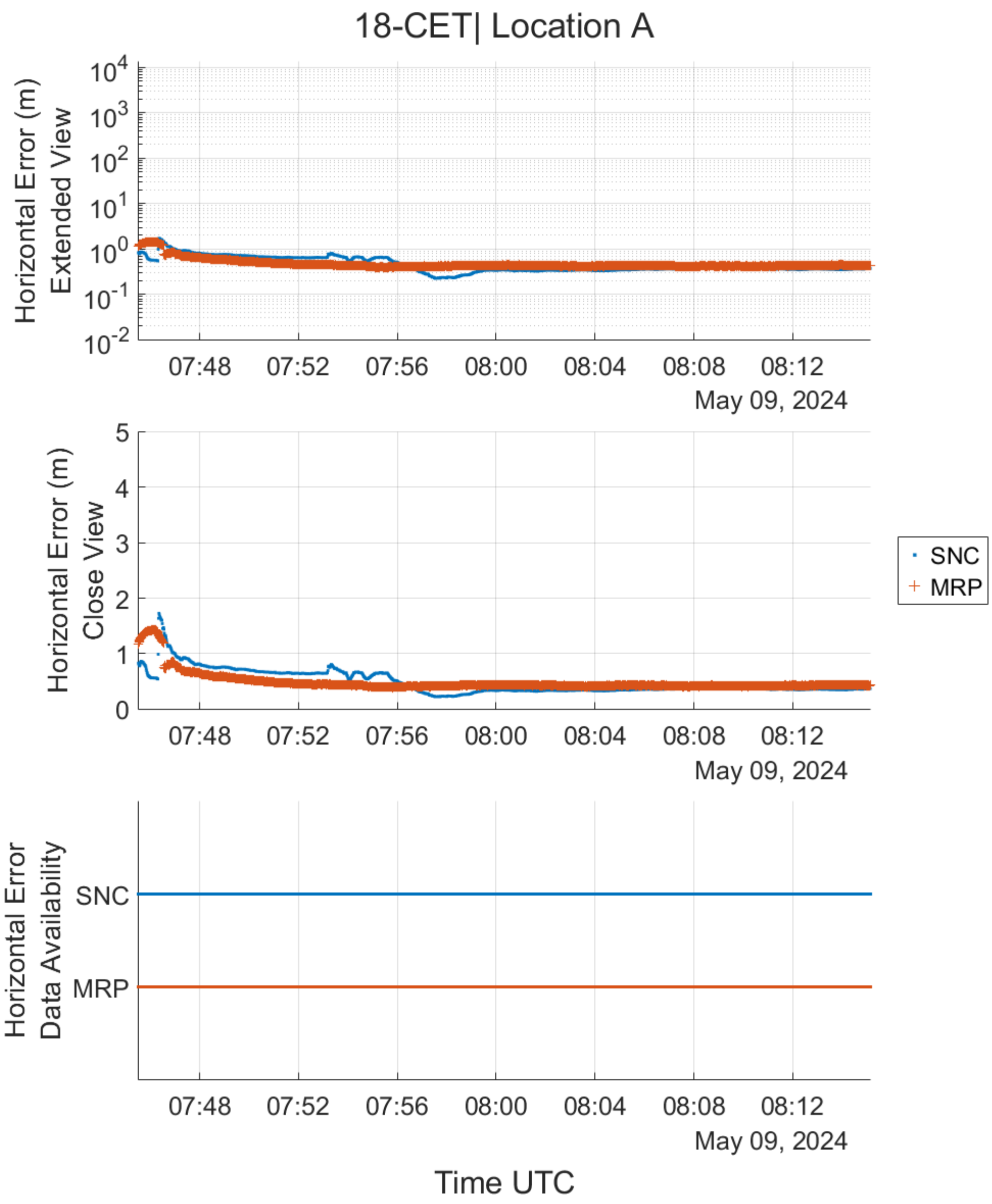


Figure 69. Horizontal position errors during scenario 18-CET

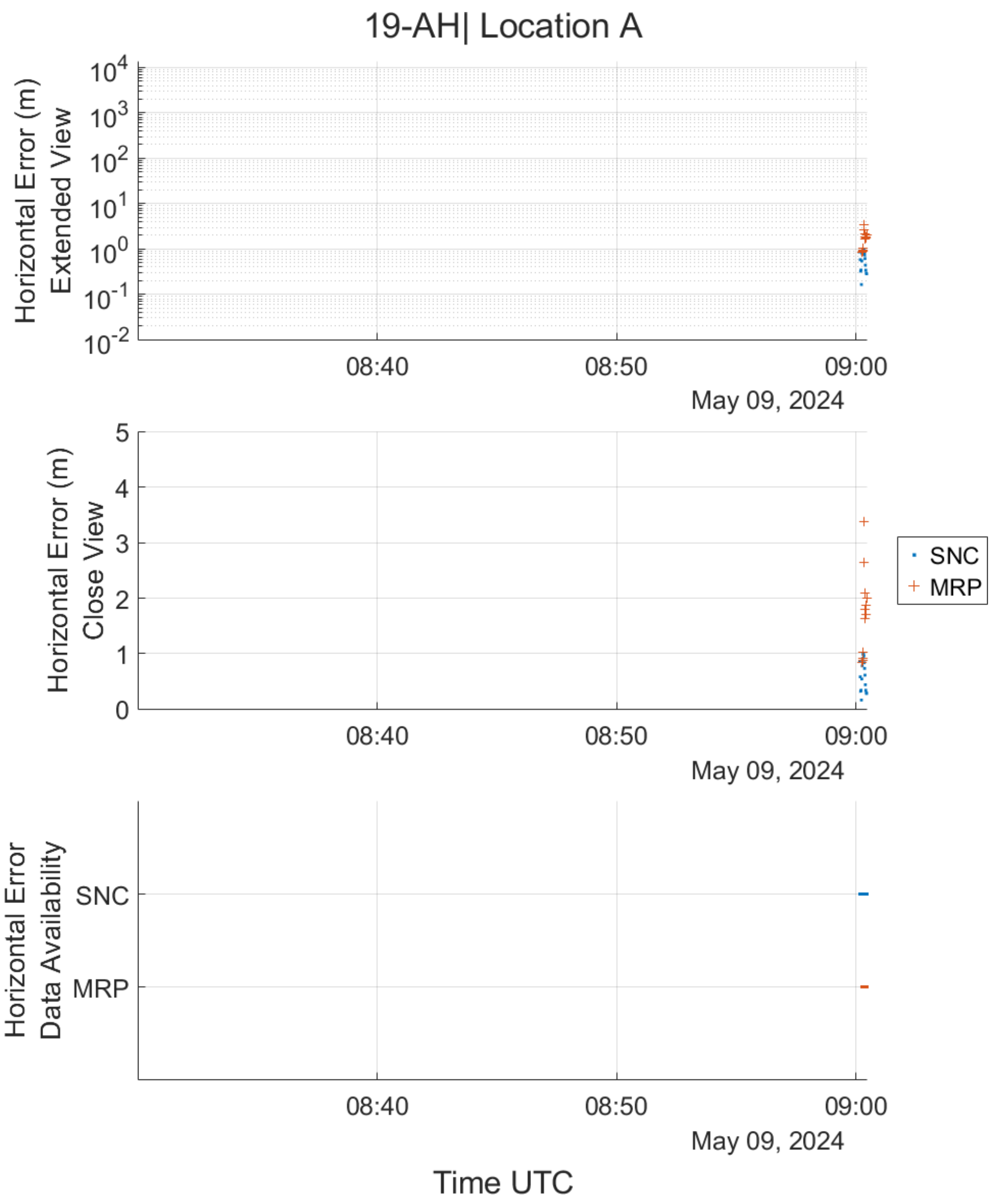


Figure 70. Horizontal position errors during scenario 19-AH

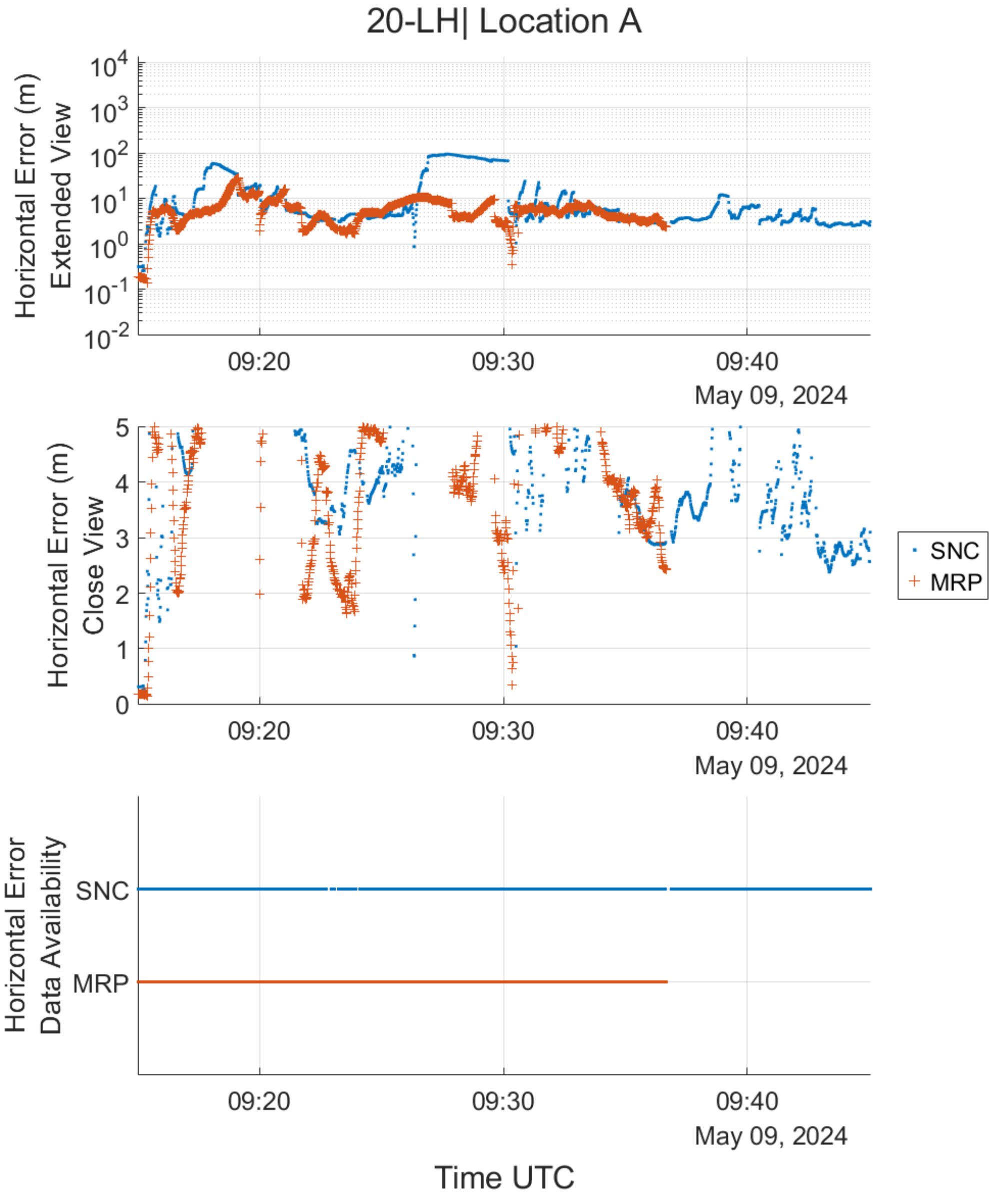


Figure 71. Horizontal position errors during scenario 20-LH

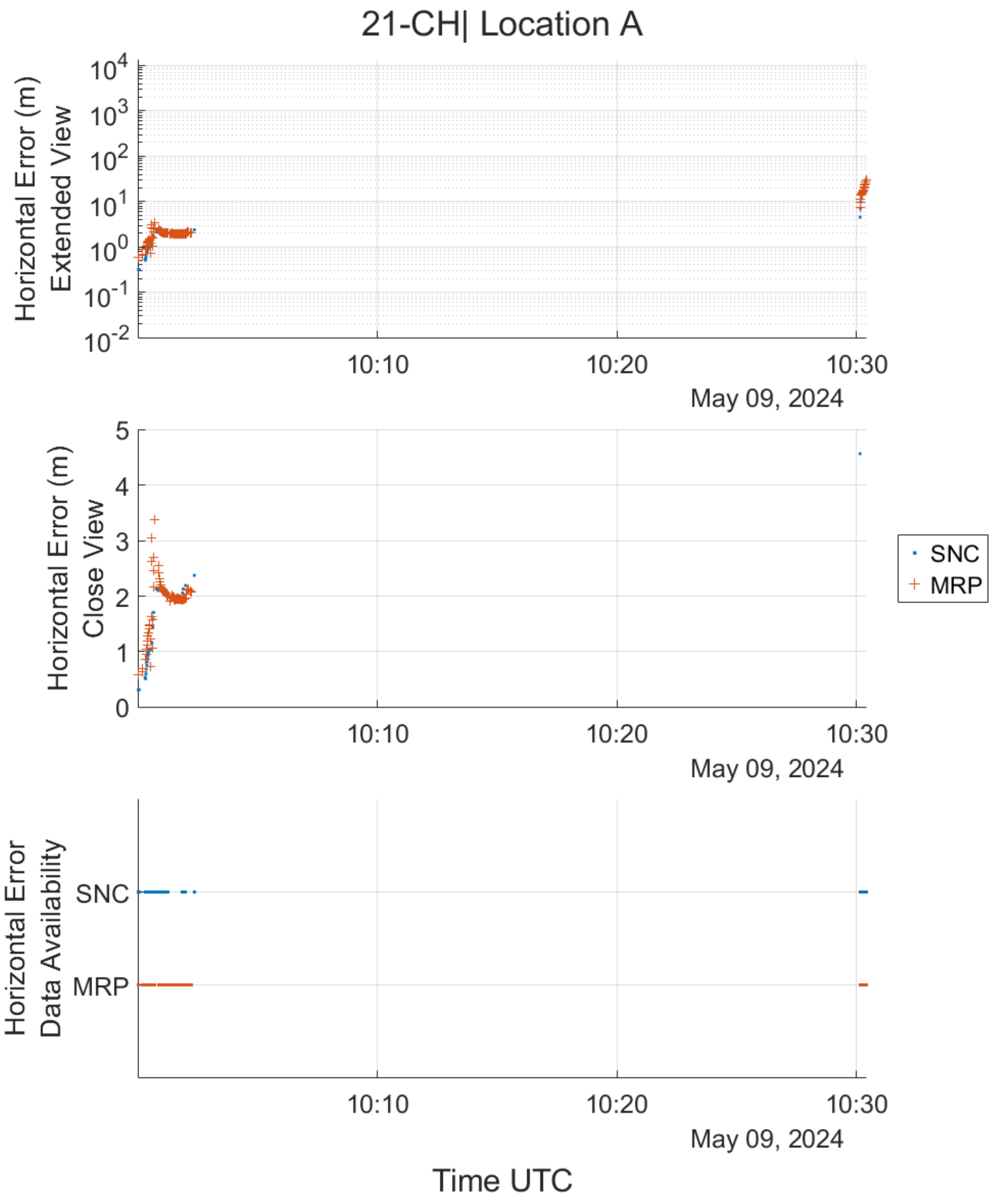


Figure 72. Horizontal position errors during scenario 21-CH

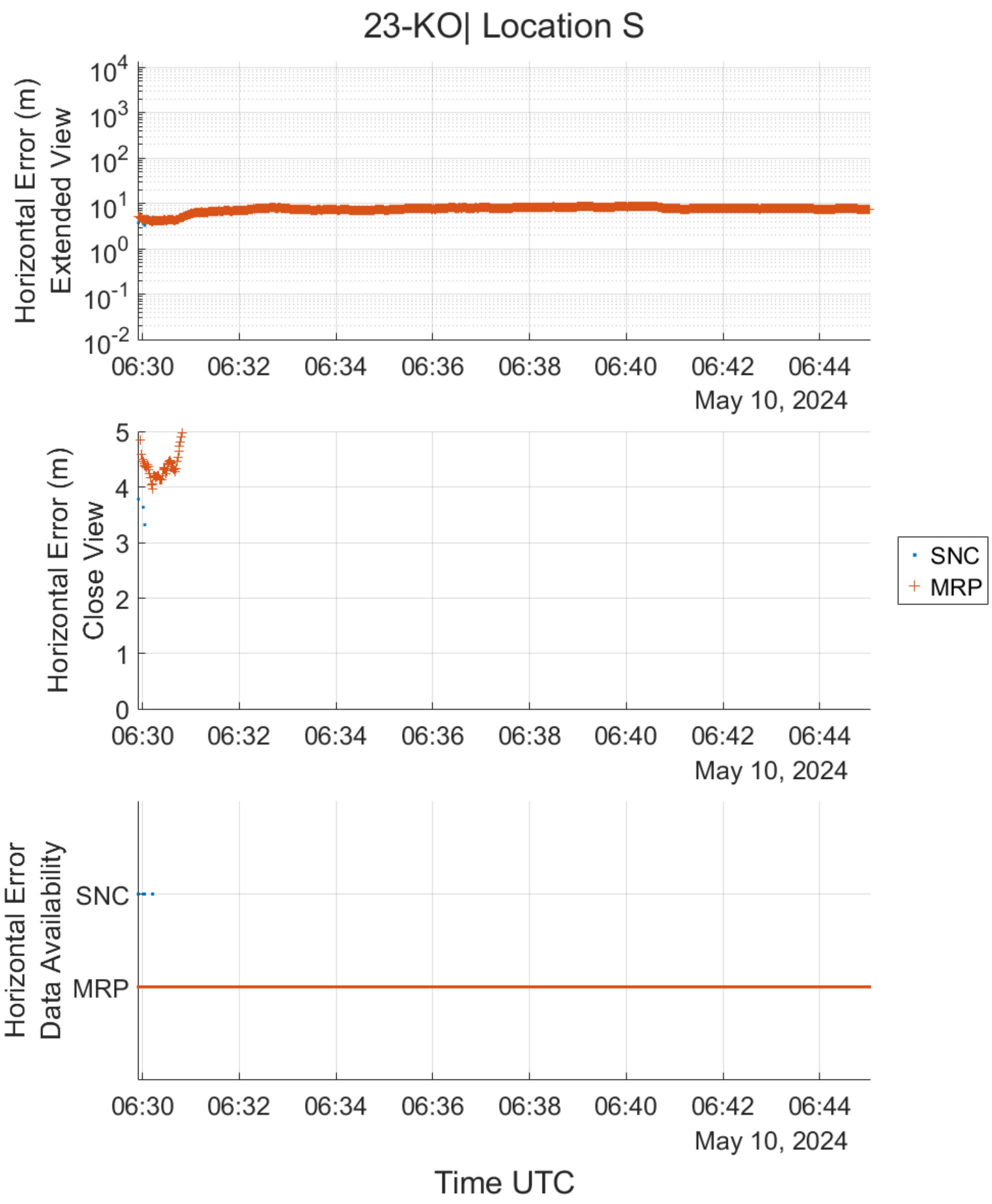


Figure 73. Horizontal position errors during scenario 23-KO

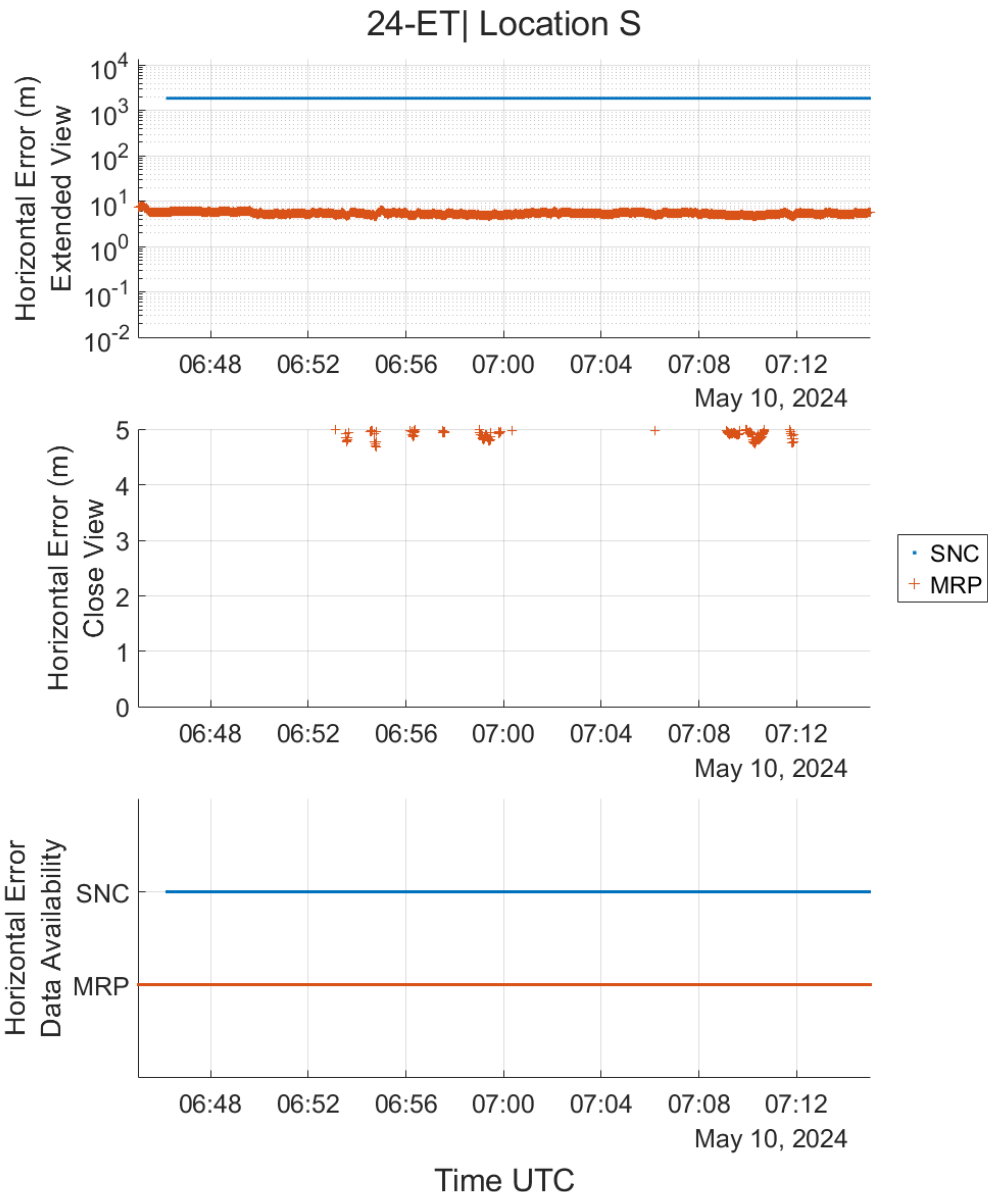


Figure 74. Horizontal position errors during scenario 24-ET

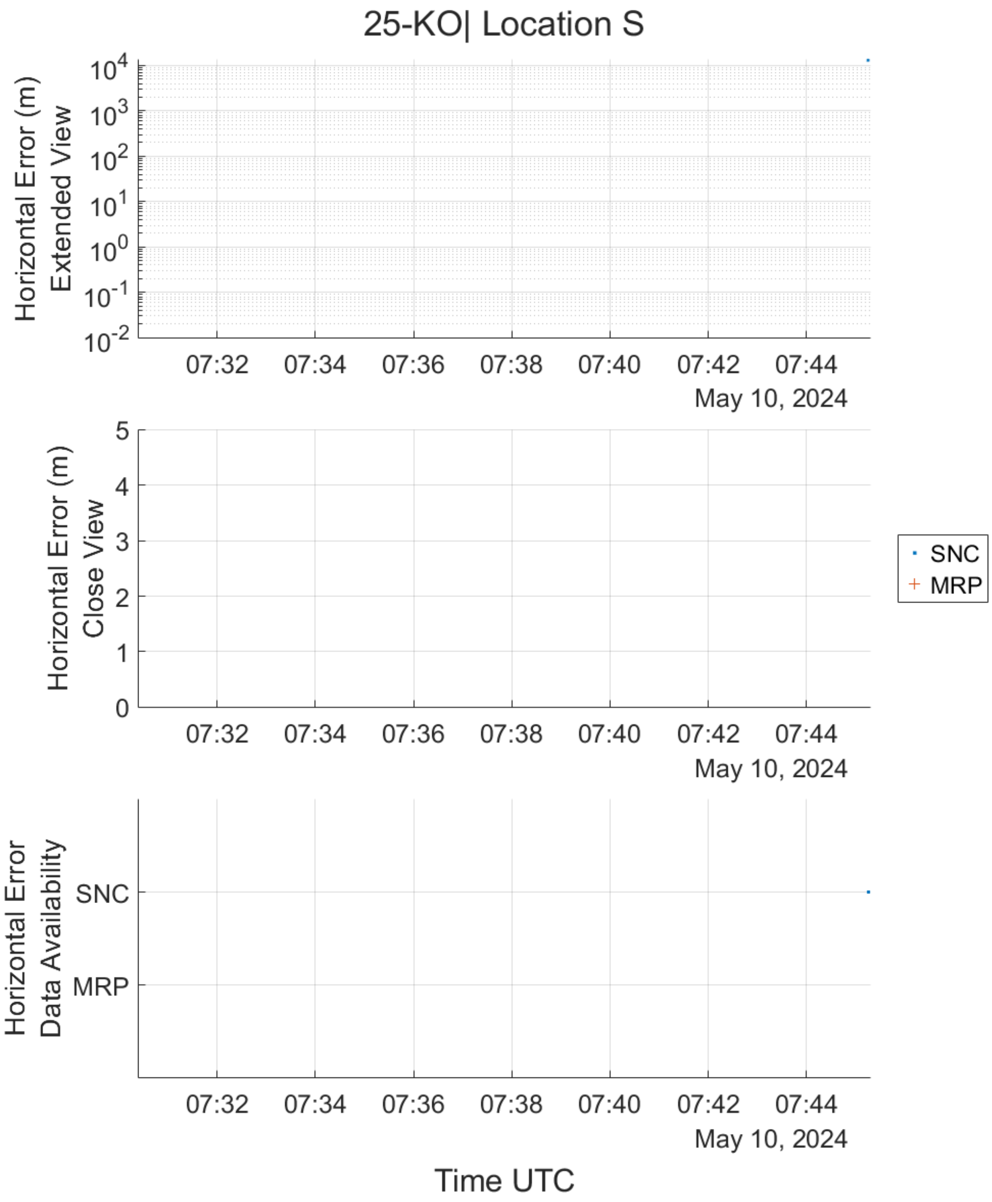


Figure 75. Horizontal position errors during scenario 25-KO

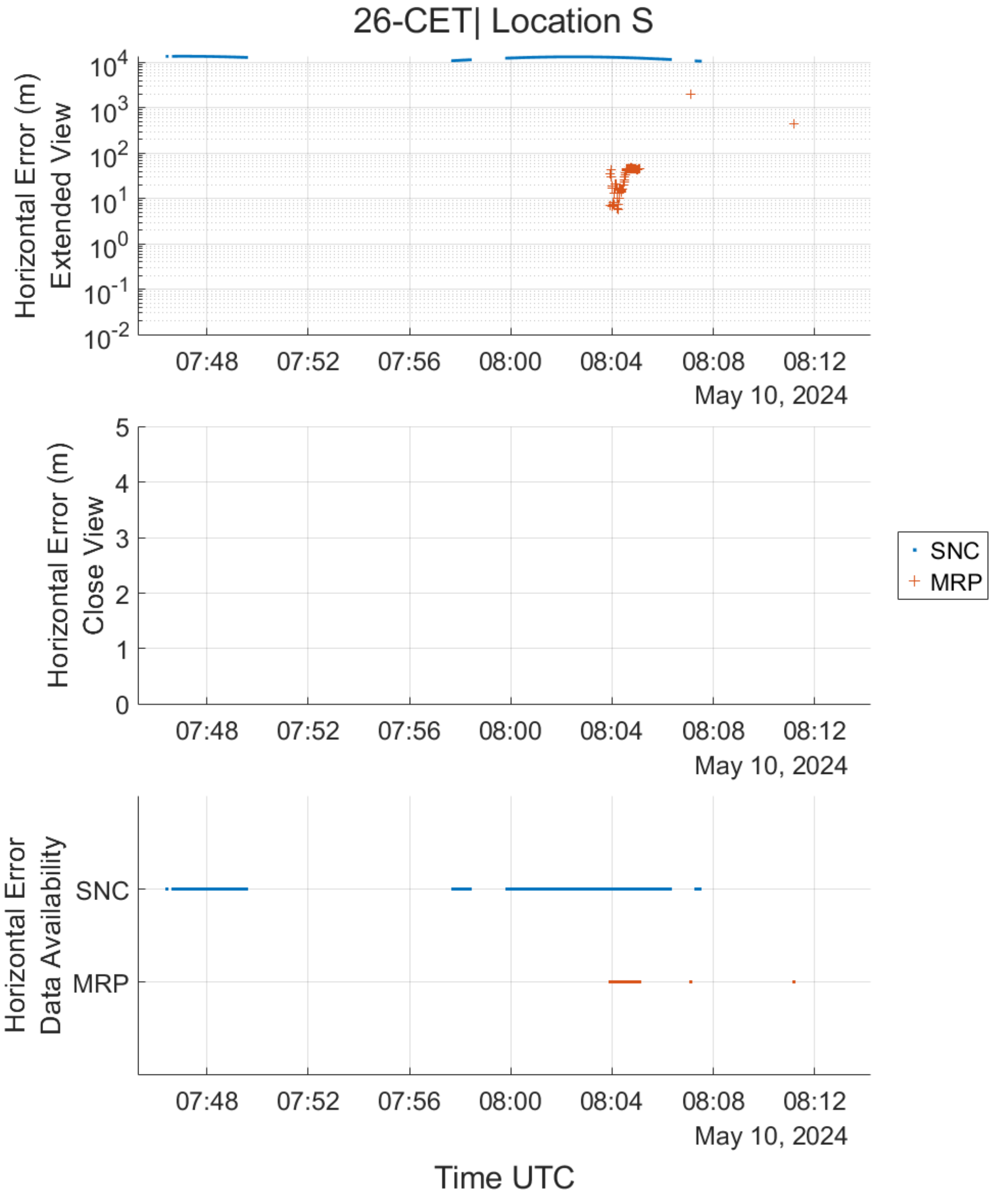


Figure 76. Horizontal position errors during scenario 26-CET

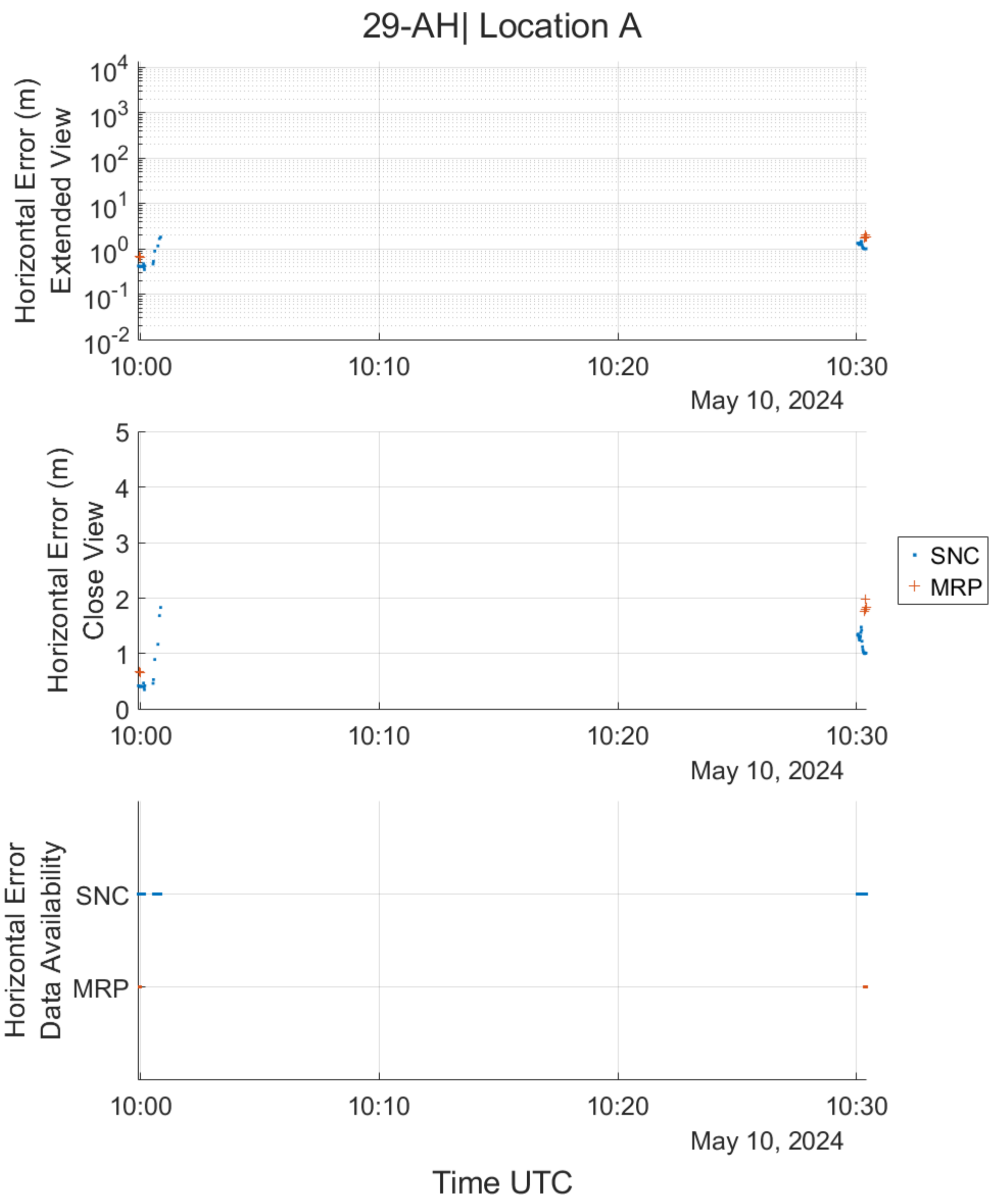


Figure 77. Horizontal position errors during scenario 29-AH

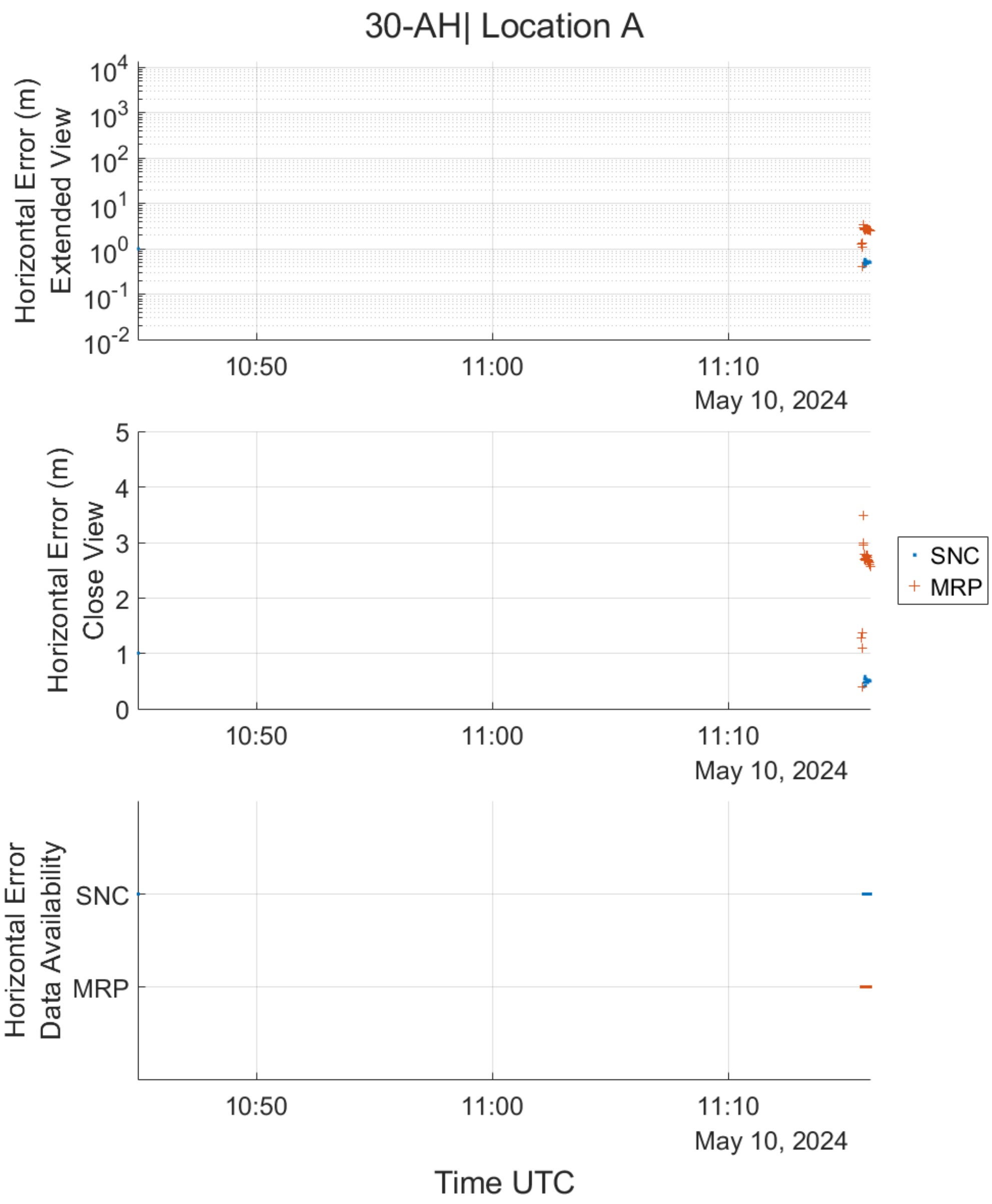


Figure 78. Horizontal position errors during scenario 30-AH

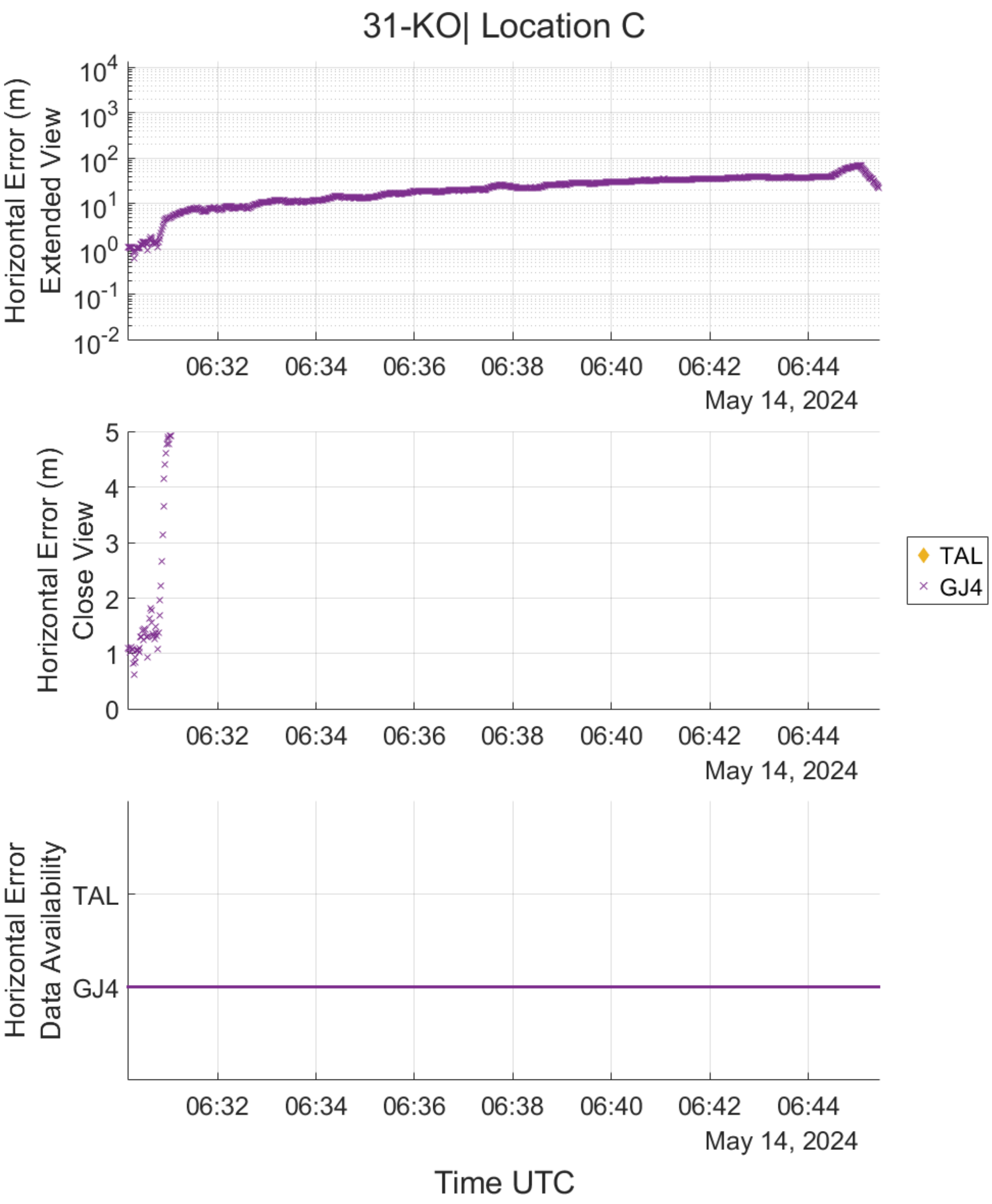


Figure 79. Horizontal position errors during scenario 31-KO

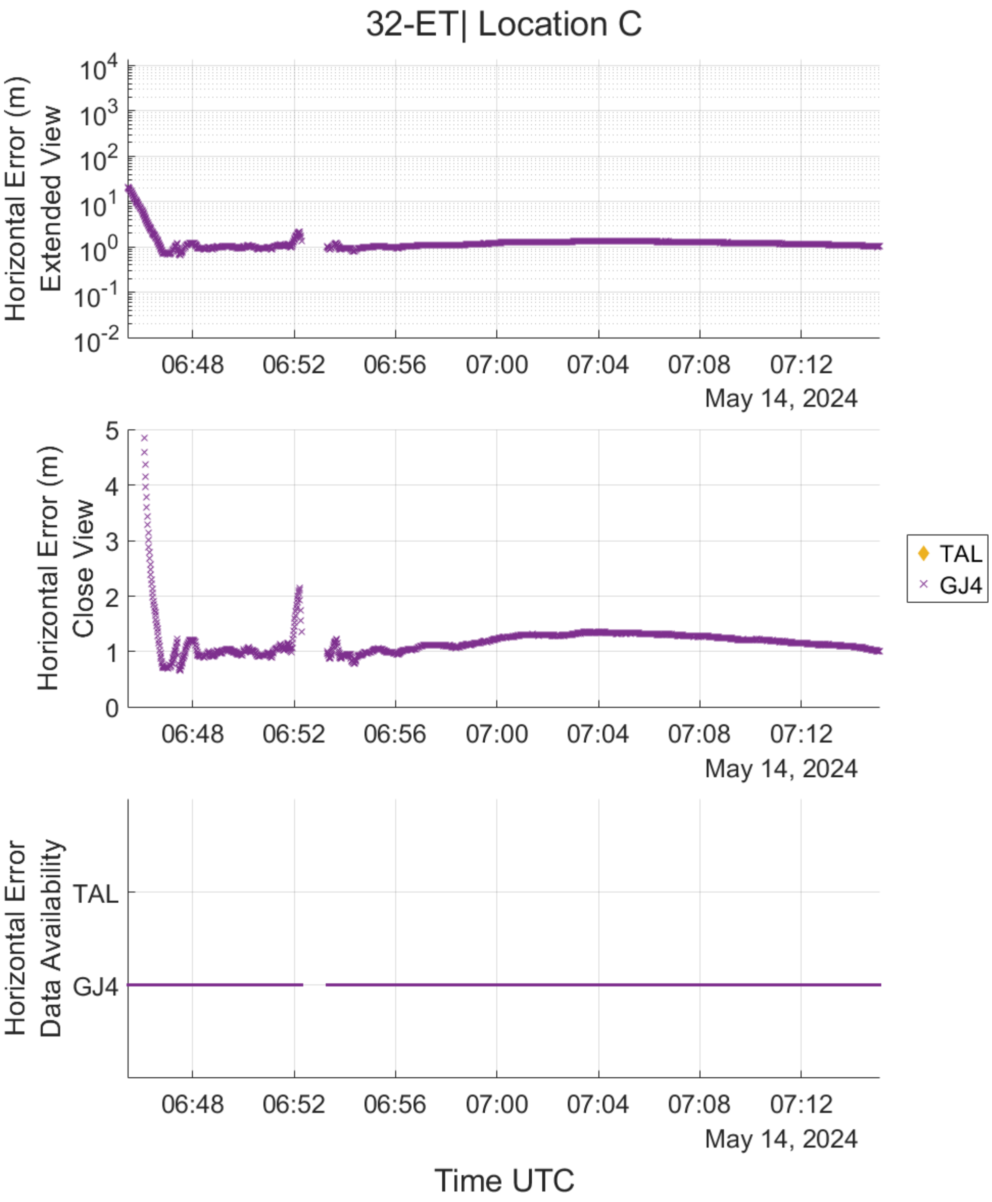


Figure 80. Horizontal position errors during scenario 32-ET

No position errors were available for any device during scenario 33-KO.

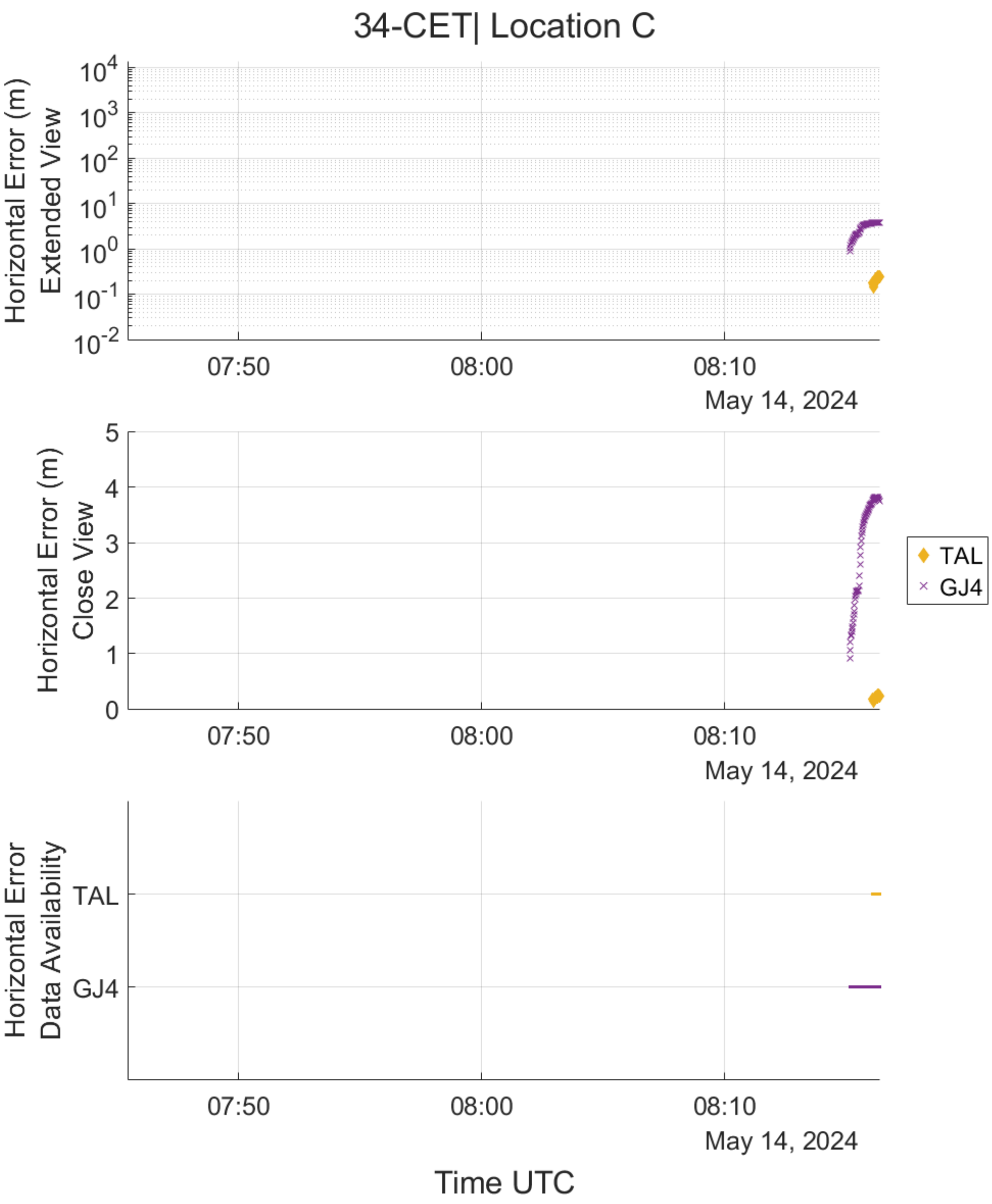


Figure 81. Horizontal position errors during scenario 34-CET

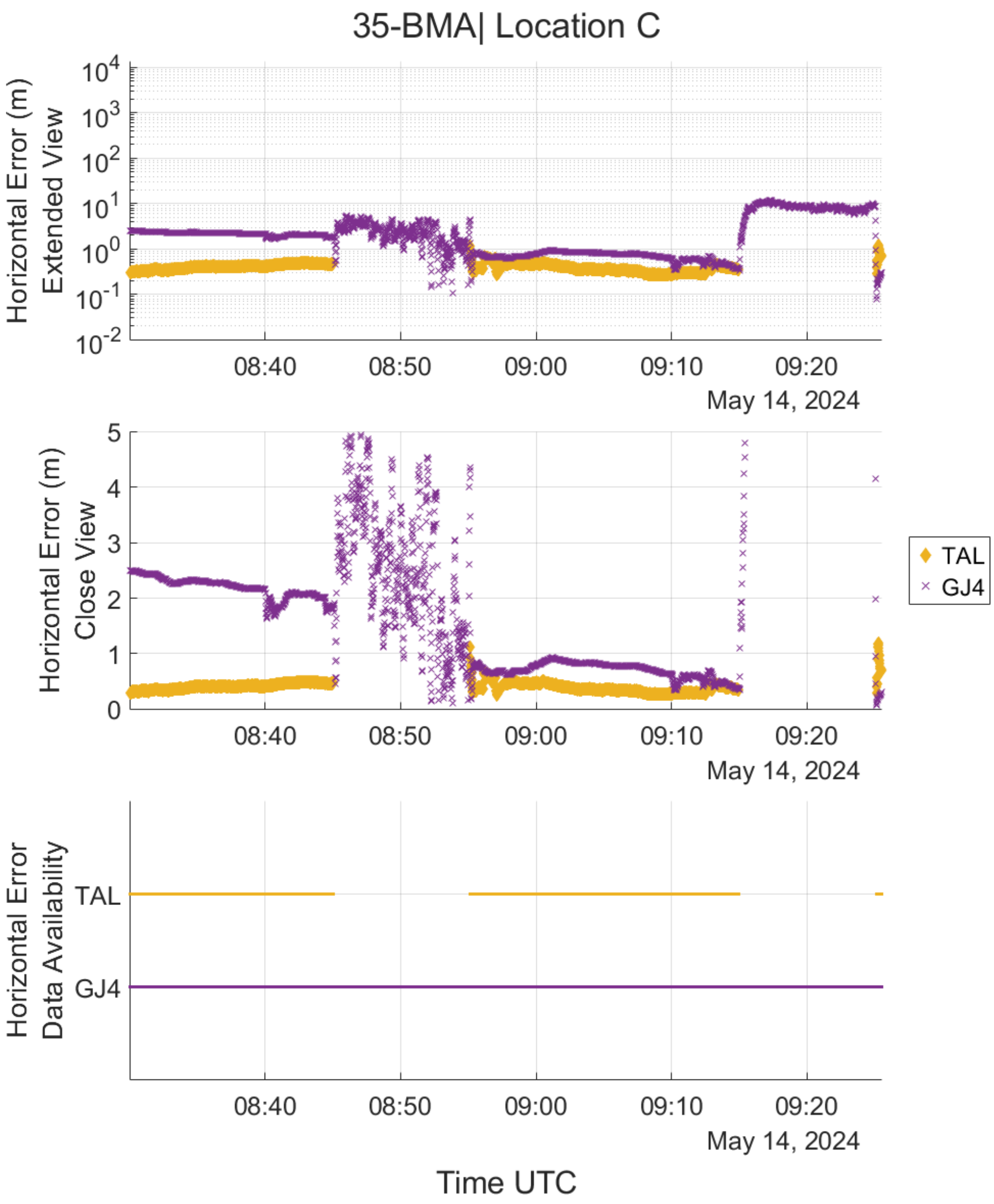


Figure 82. Horizontal position errors during scenario 35-BMA

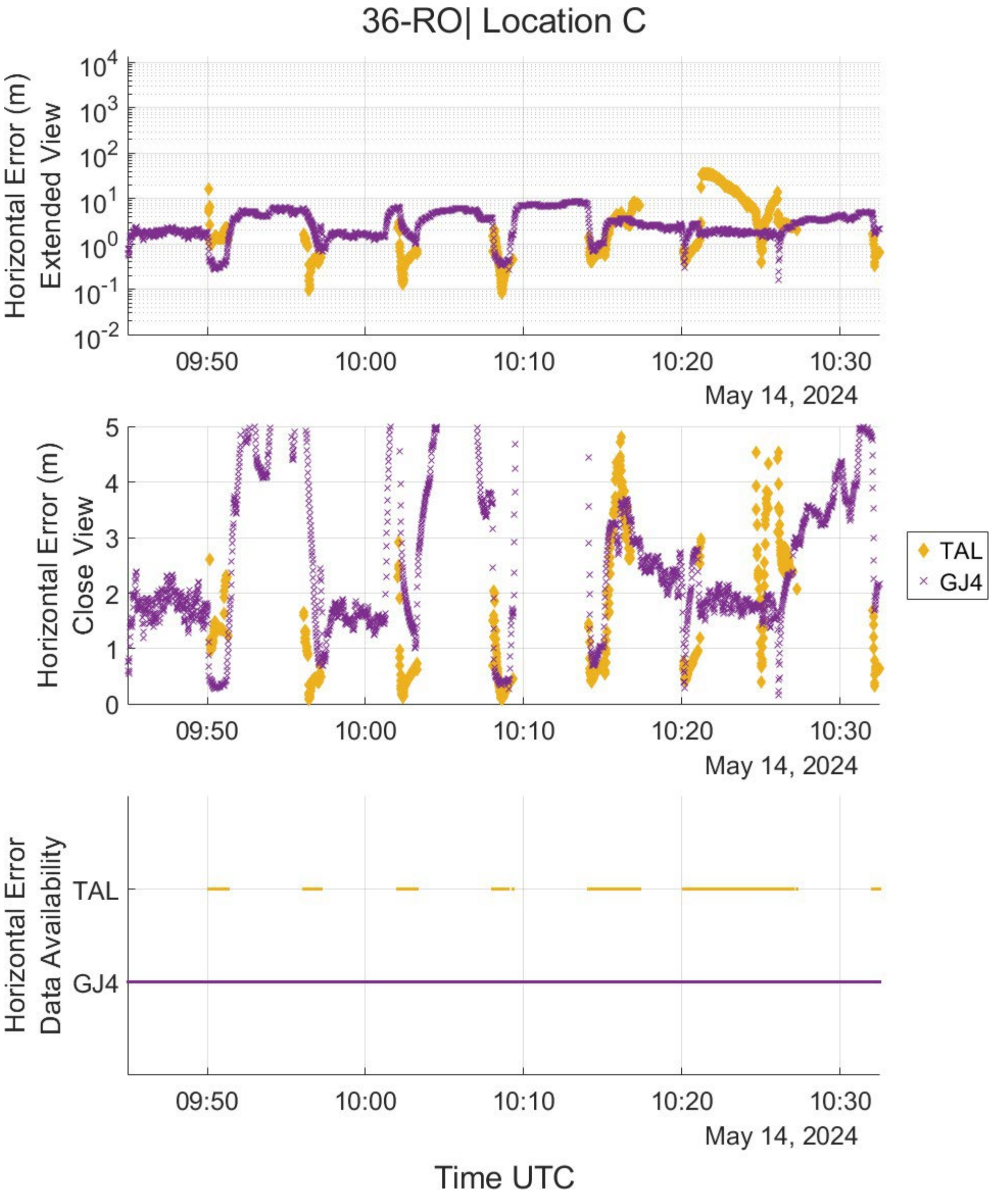


Figure 83. Horizontal position errors during scenario 36-RO

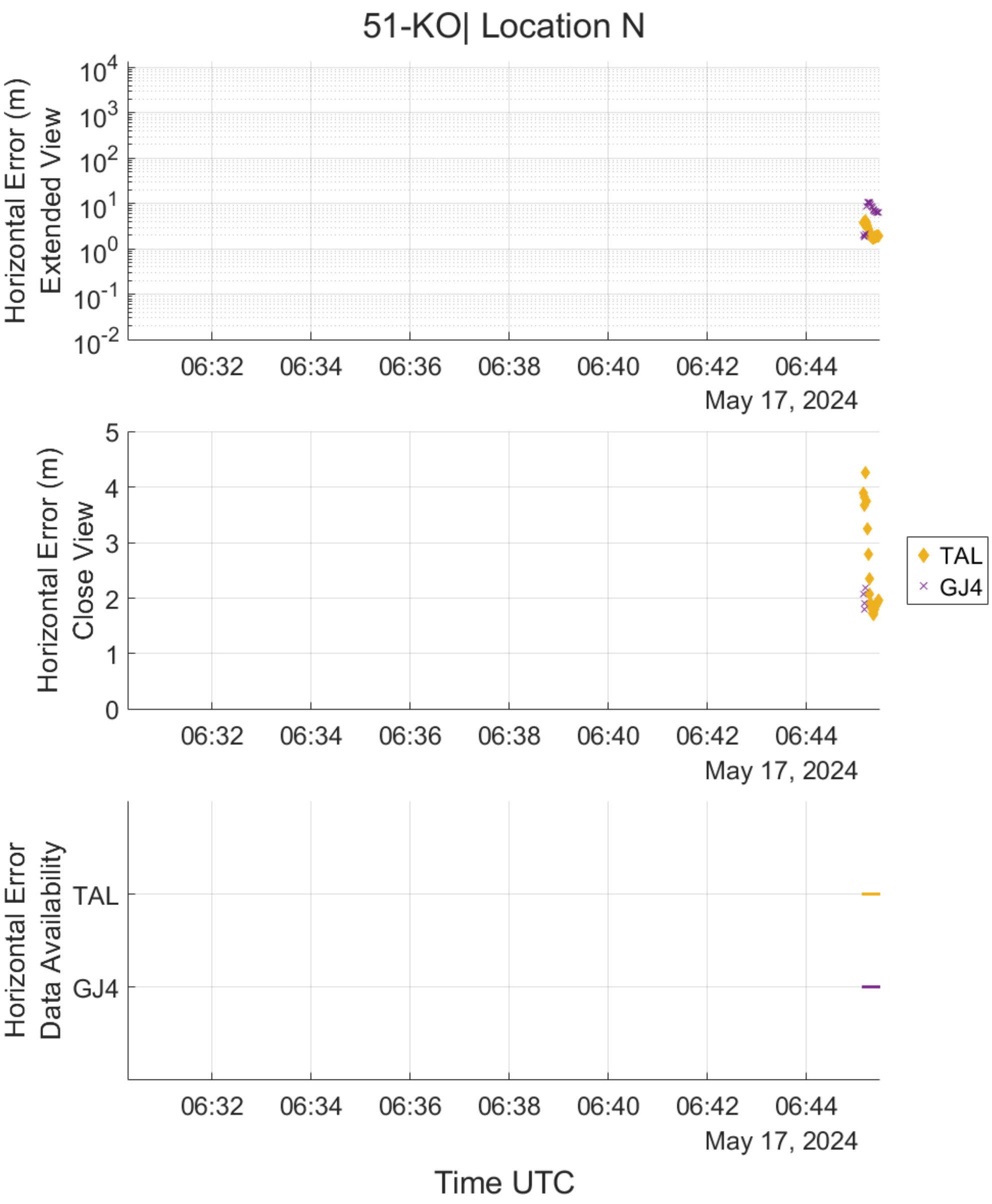


Figure 84. Horizontal position errors during scenario 51-KO

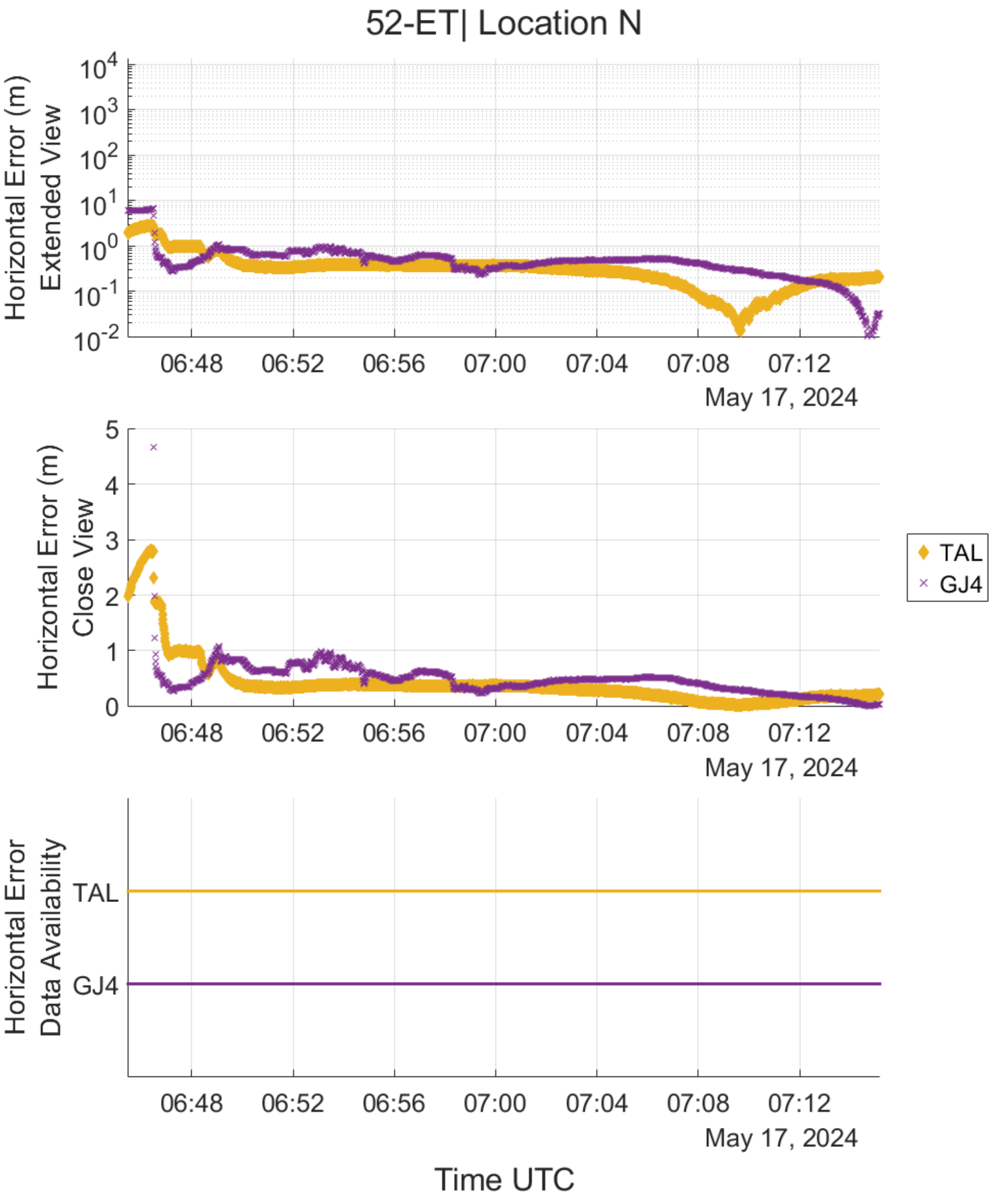


Figure 85. Horizontal position errors during scenario 52-ET

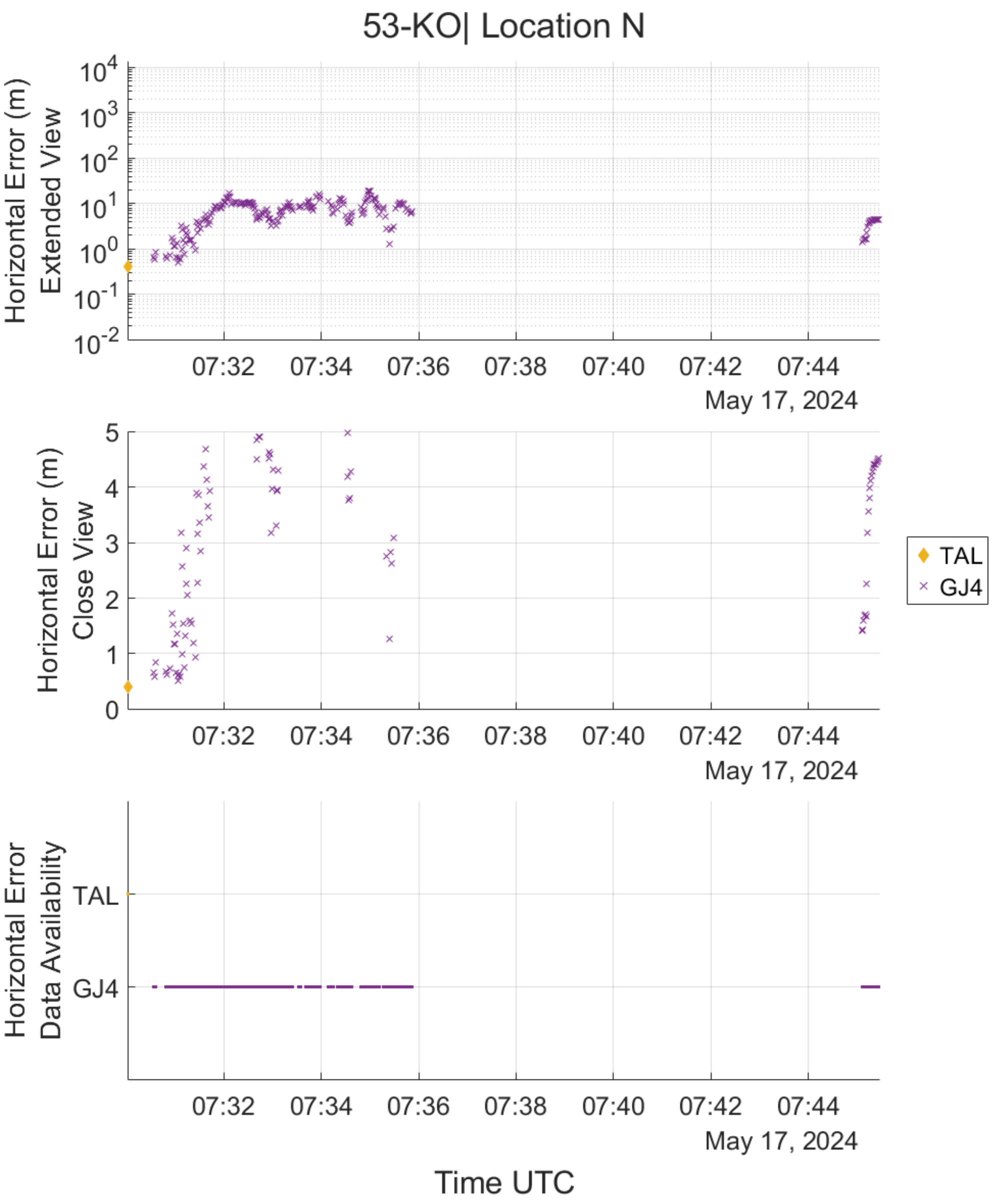


Figure 86. Horizontal position errors during scenario 53-KO

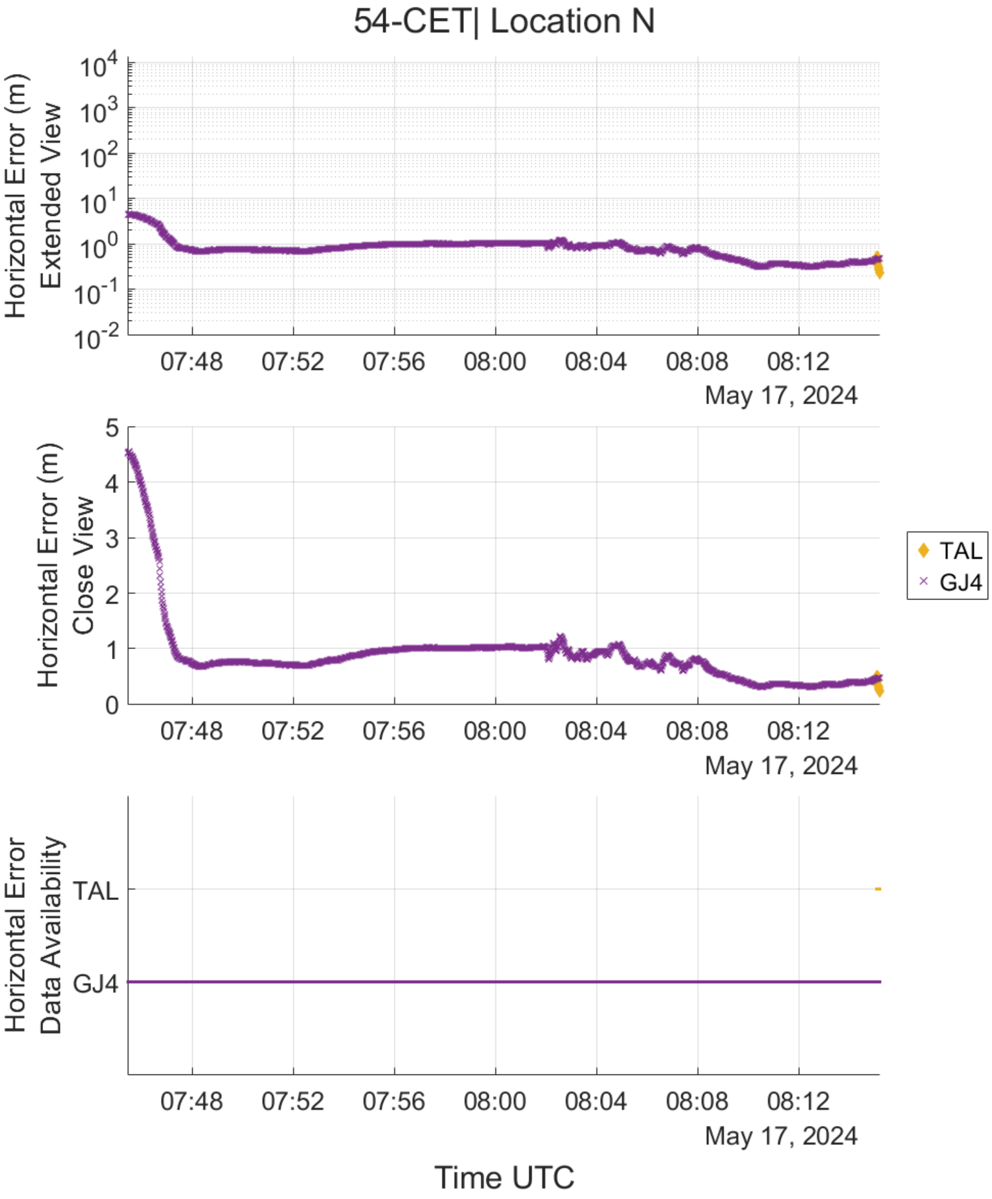


Figure 87. Horizontal position errors during scenario 54-CET

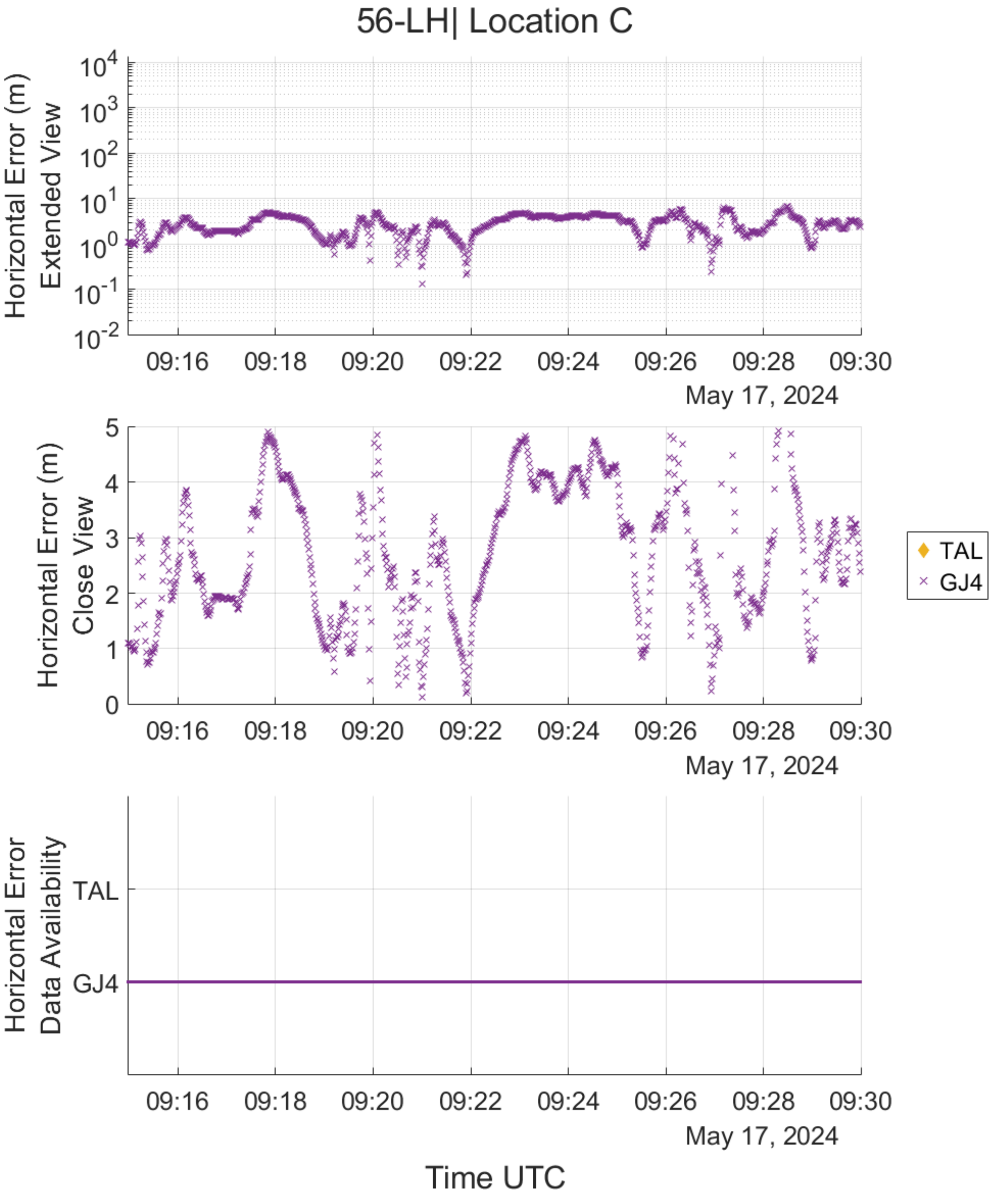


Figure 88. Horizontal position errors during scenario 56-LH

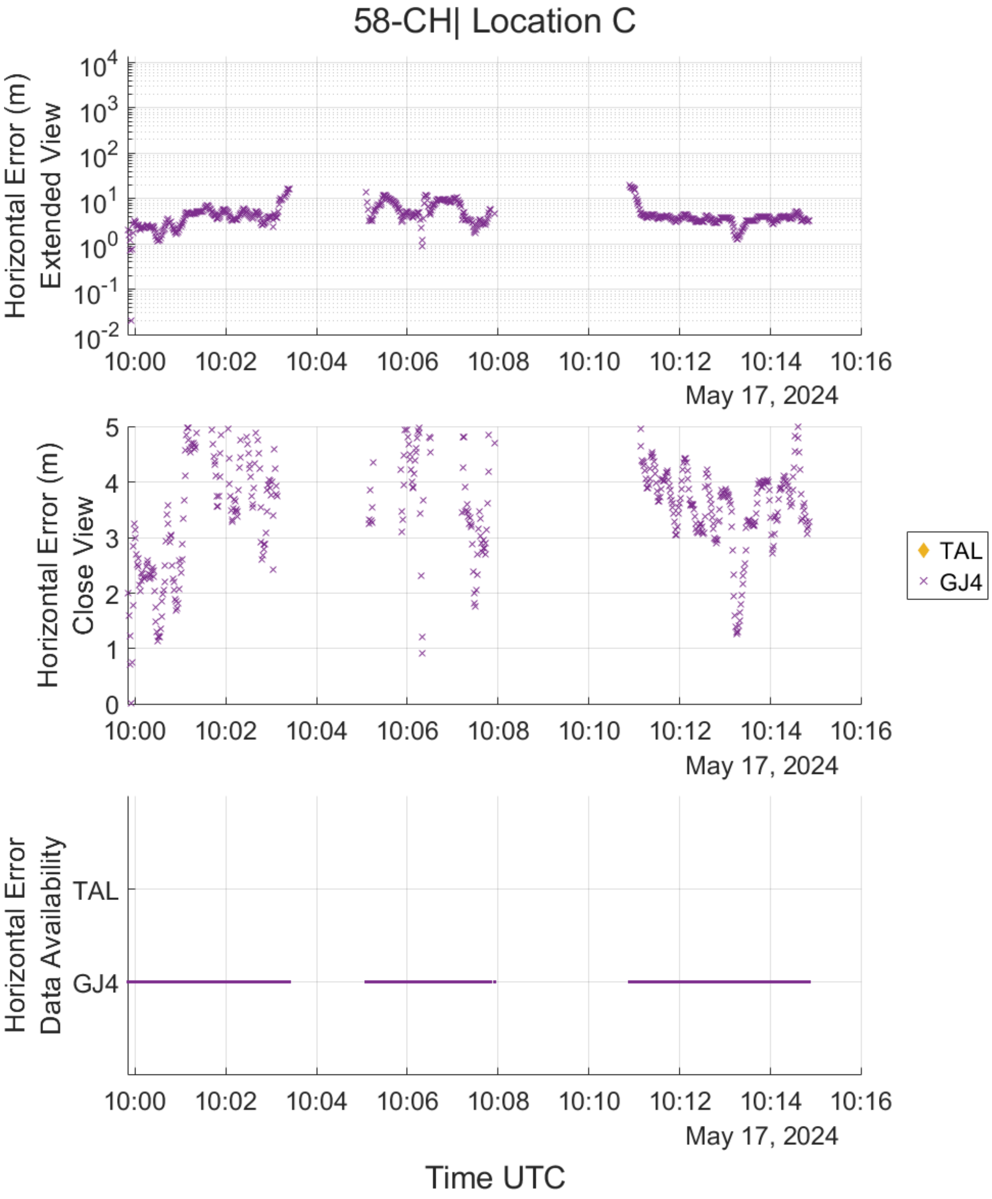


Figure 89. Horizontal position errors during scenario 58-CH

Appendix D: NAVFEST Static Recovery Analysis Time Series Plots

This appendix contains the time series plots for the NAVFEST static recovery analysis. Each plot shows the horizontal position errors starting near the end of a scenario and extending through the recovery window. All plots are included, regardless of whether the device recovered within the recovery window.

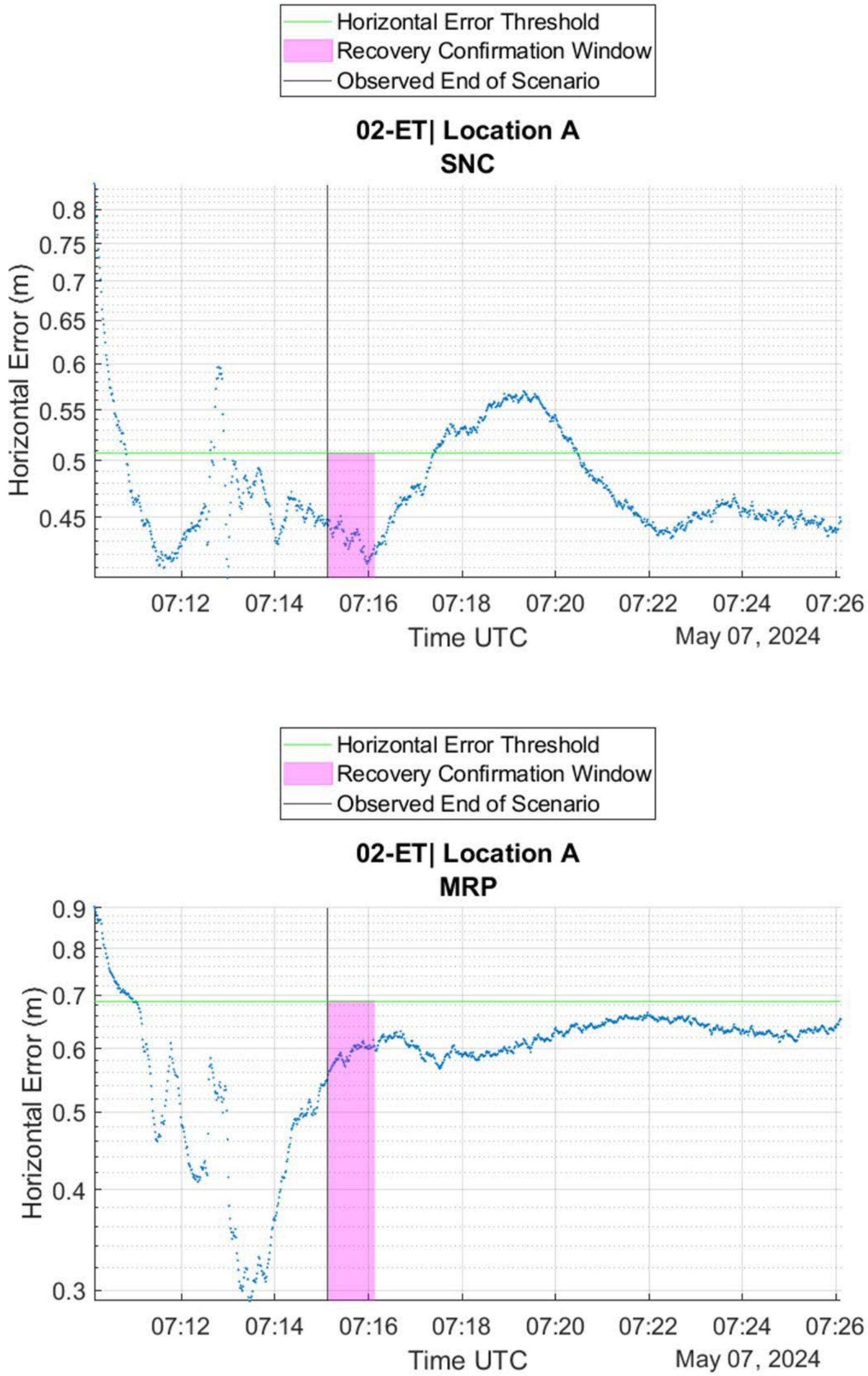


Figure 90. Static recovery analysis time series plots for scenario 02-ET

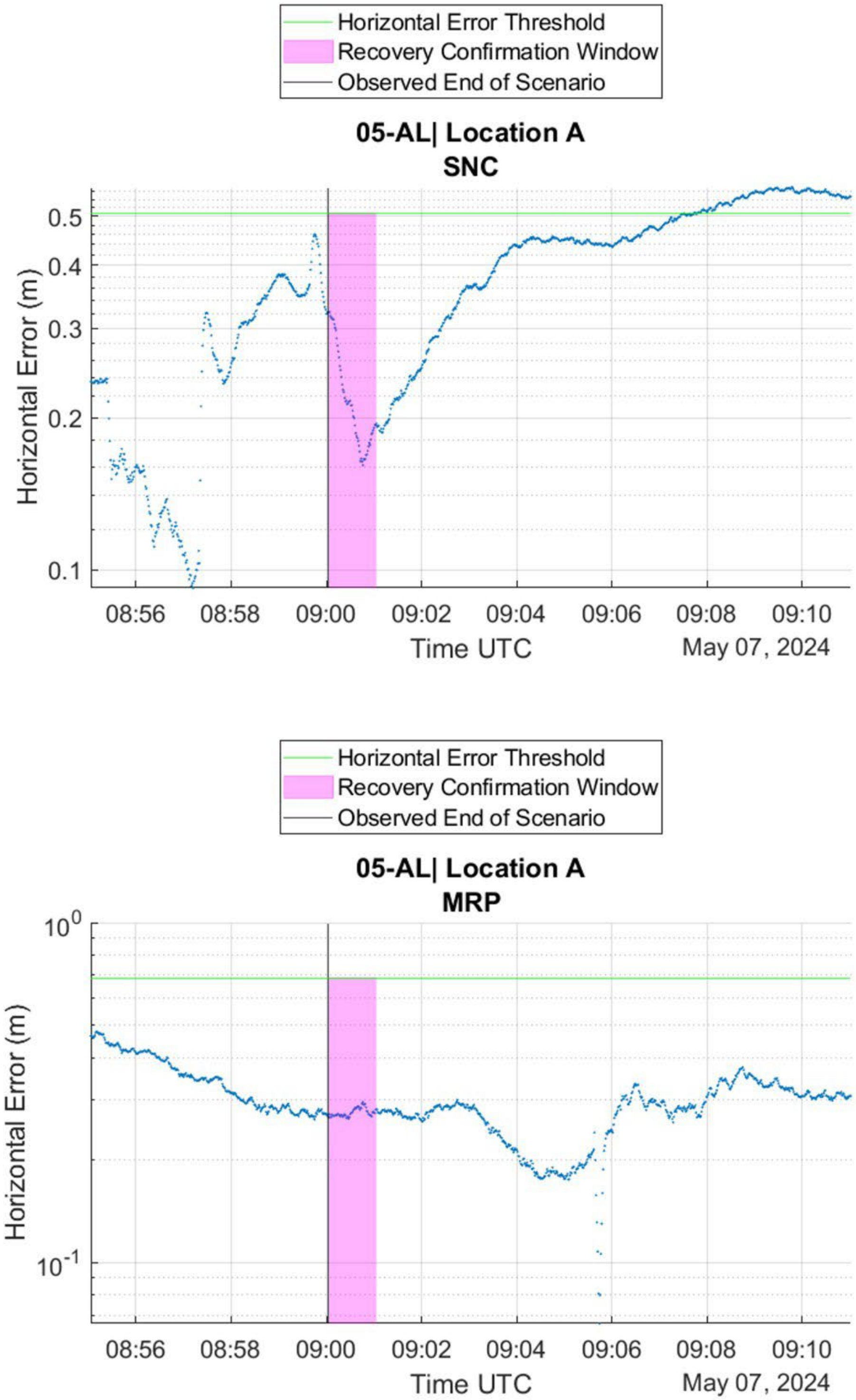


Figure 91. Static recovery analysis time series plots for scenario 05-AL

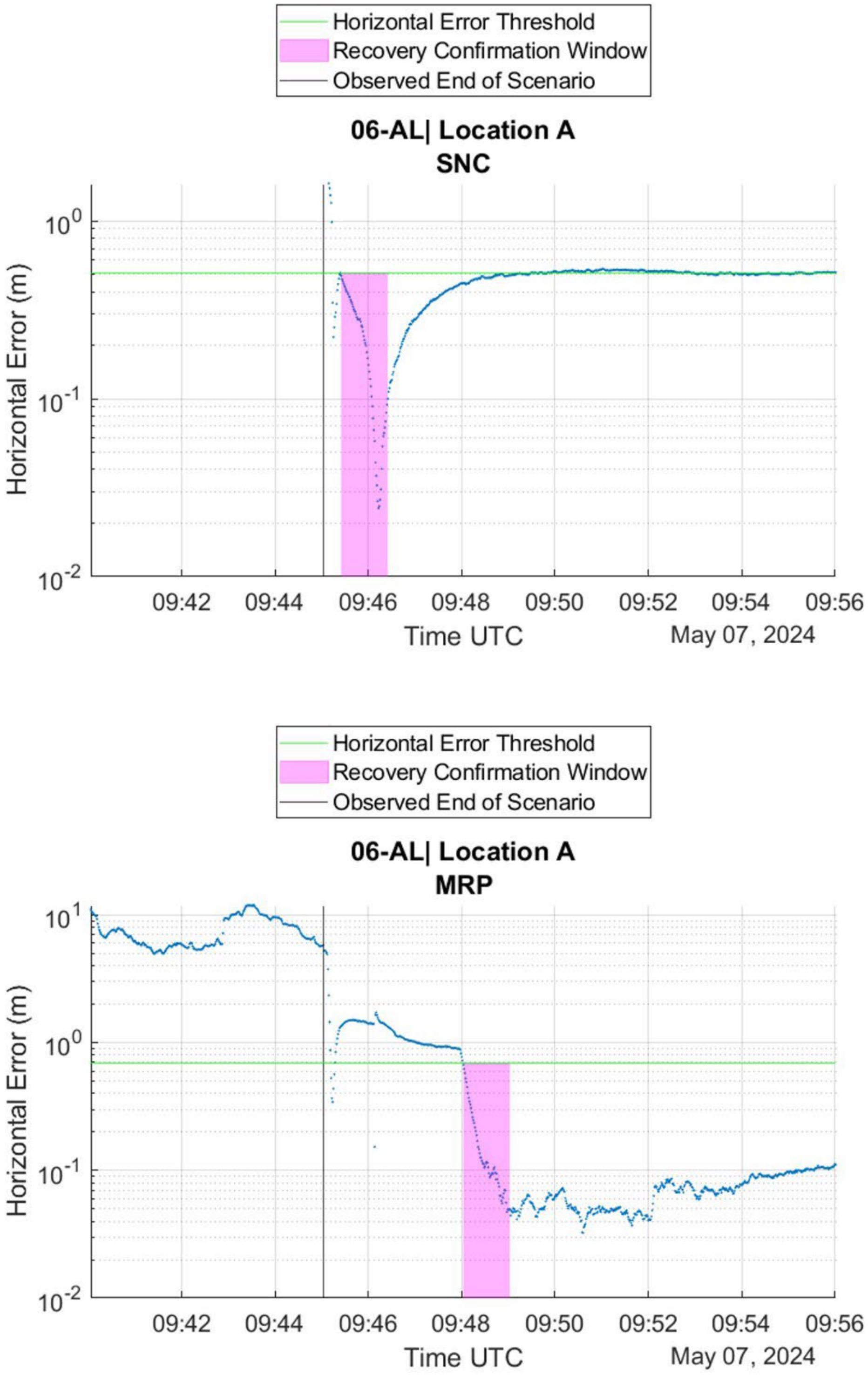
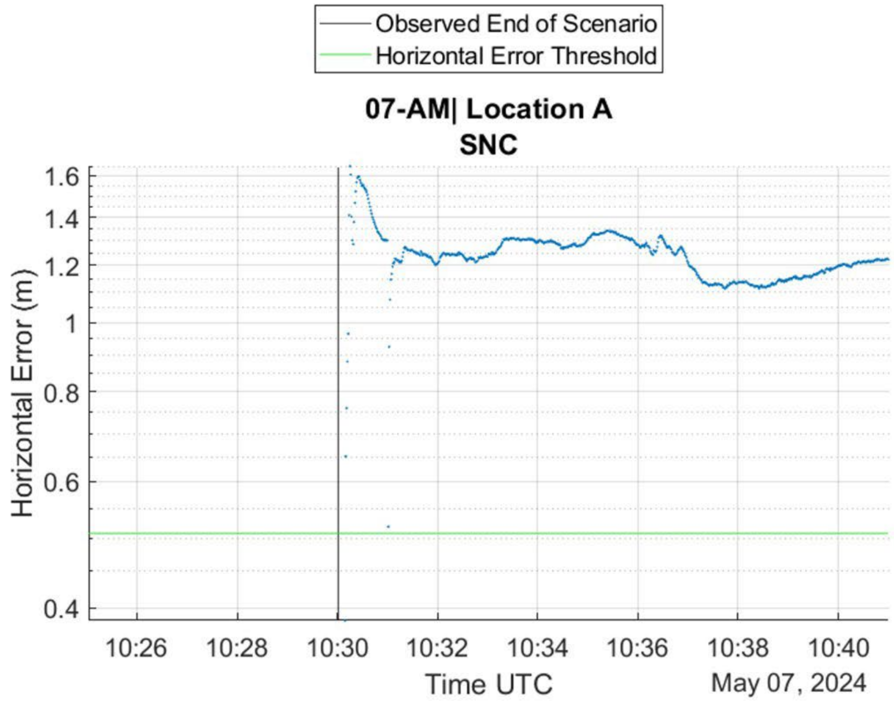


Figure 92. Static recovery analysis time series plots for scenario 06-AL



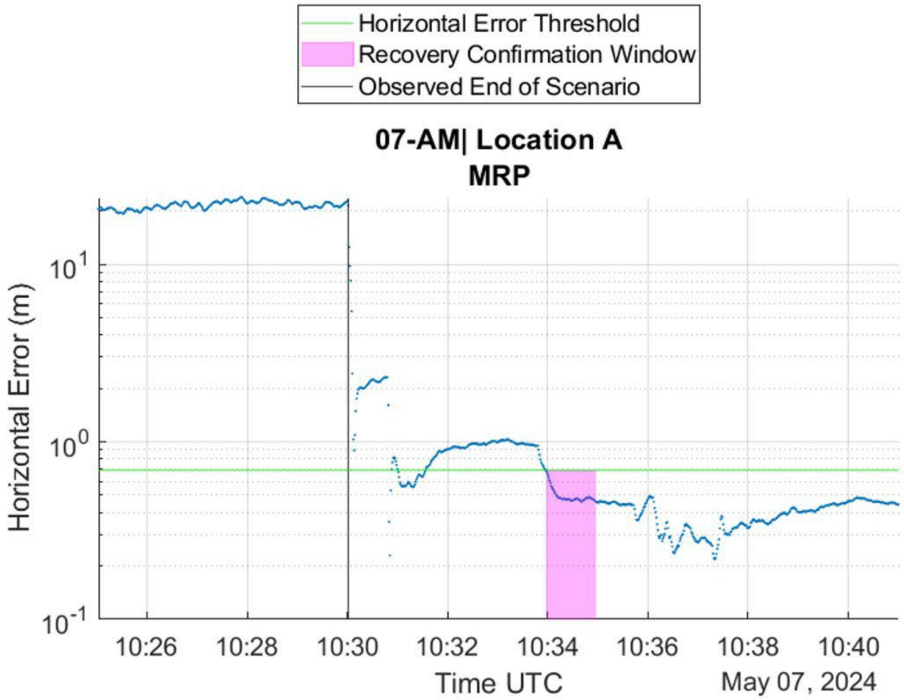


Figure 93. Static recovery analysis time series plots for scenario 07-AM

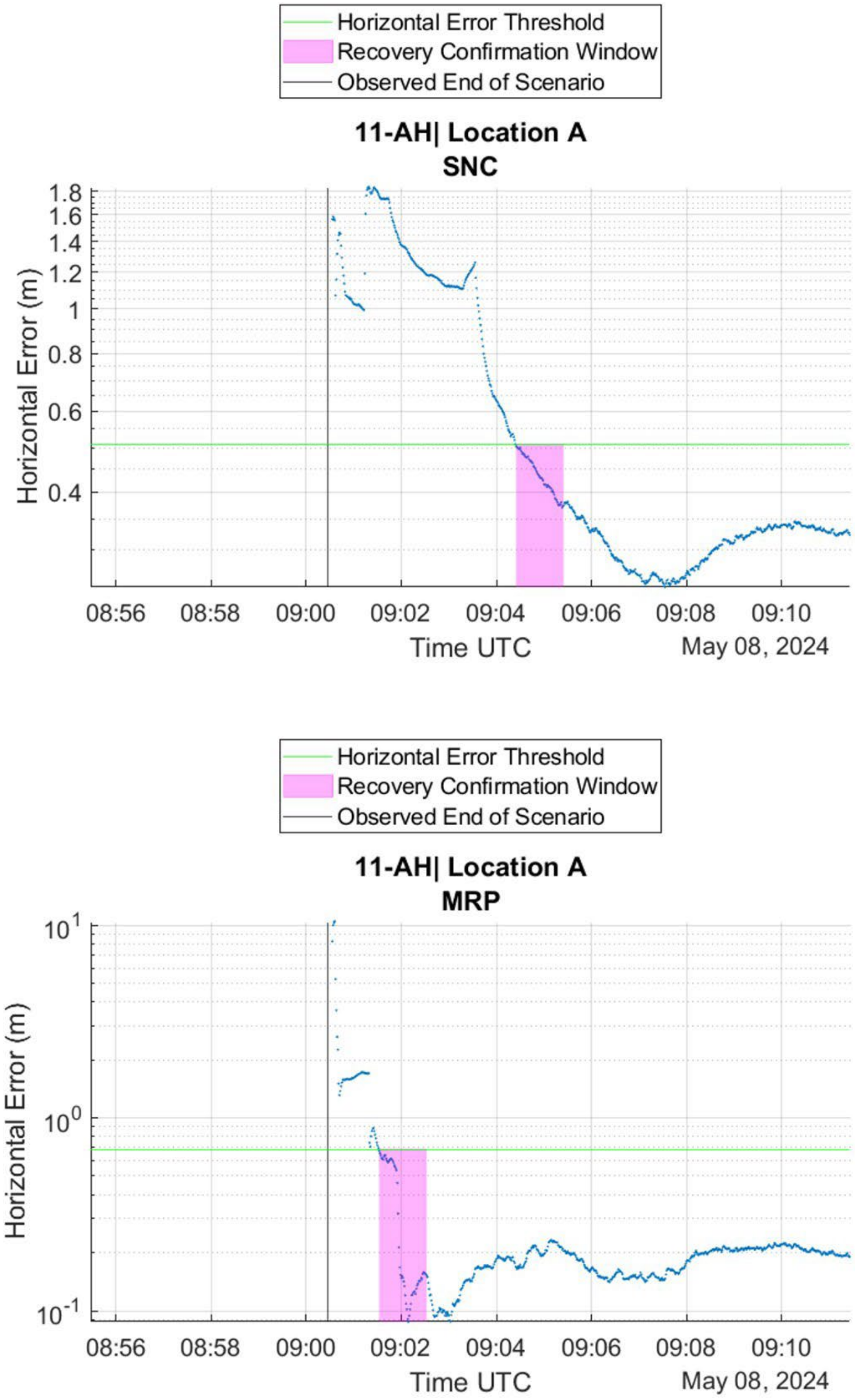
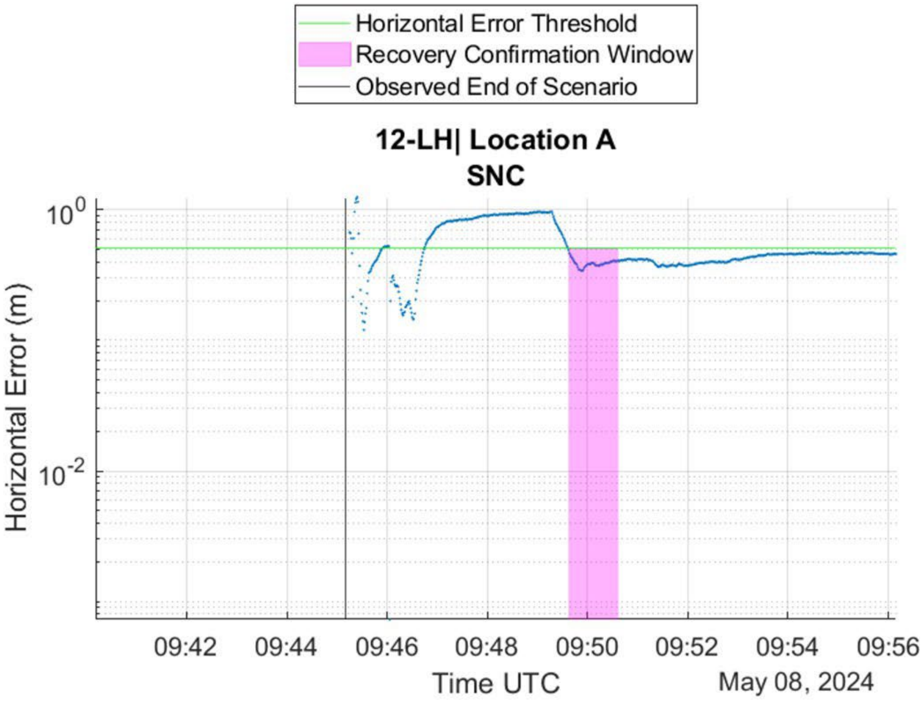


Figure 94. Static recovery analysis time series plots for scenario 11-AH



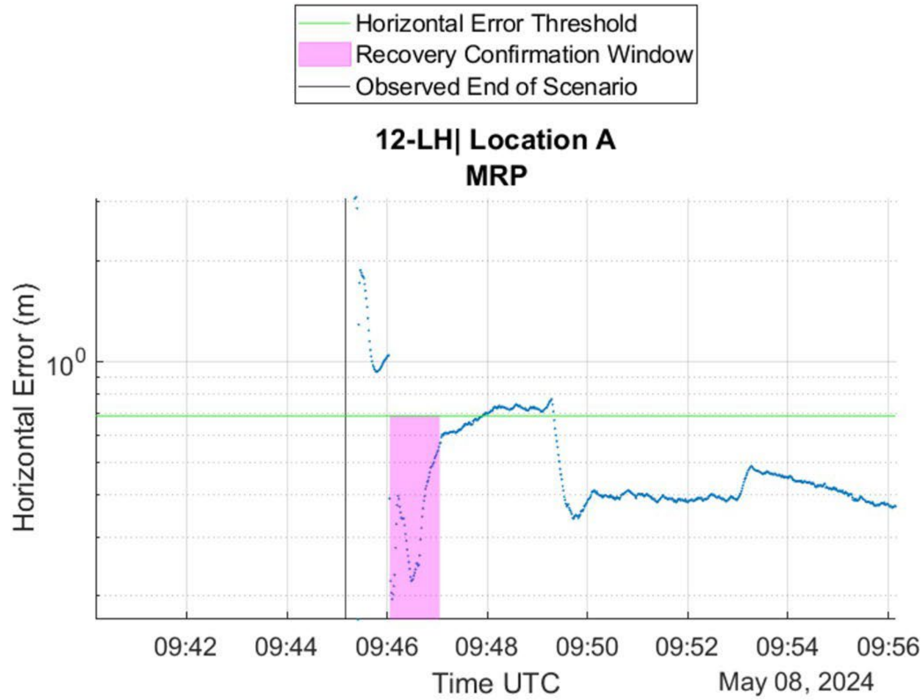


Figure 95. Static recovery analysis time series plots for scenario 12-LH

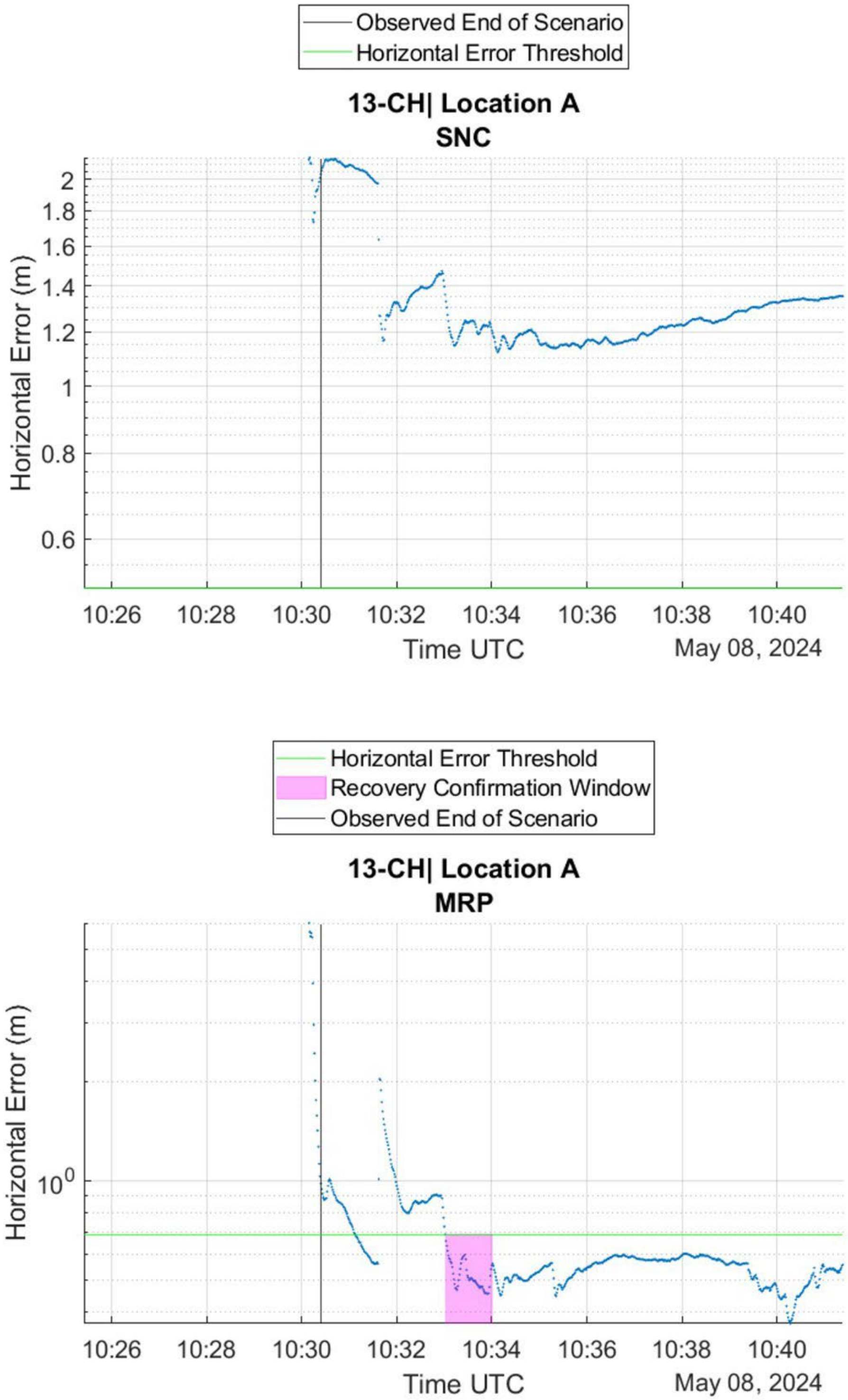


Figure 96. Static recovery analysis time series plots for scenario 13-CH

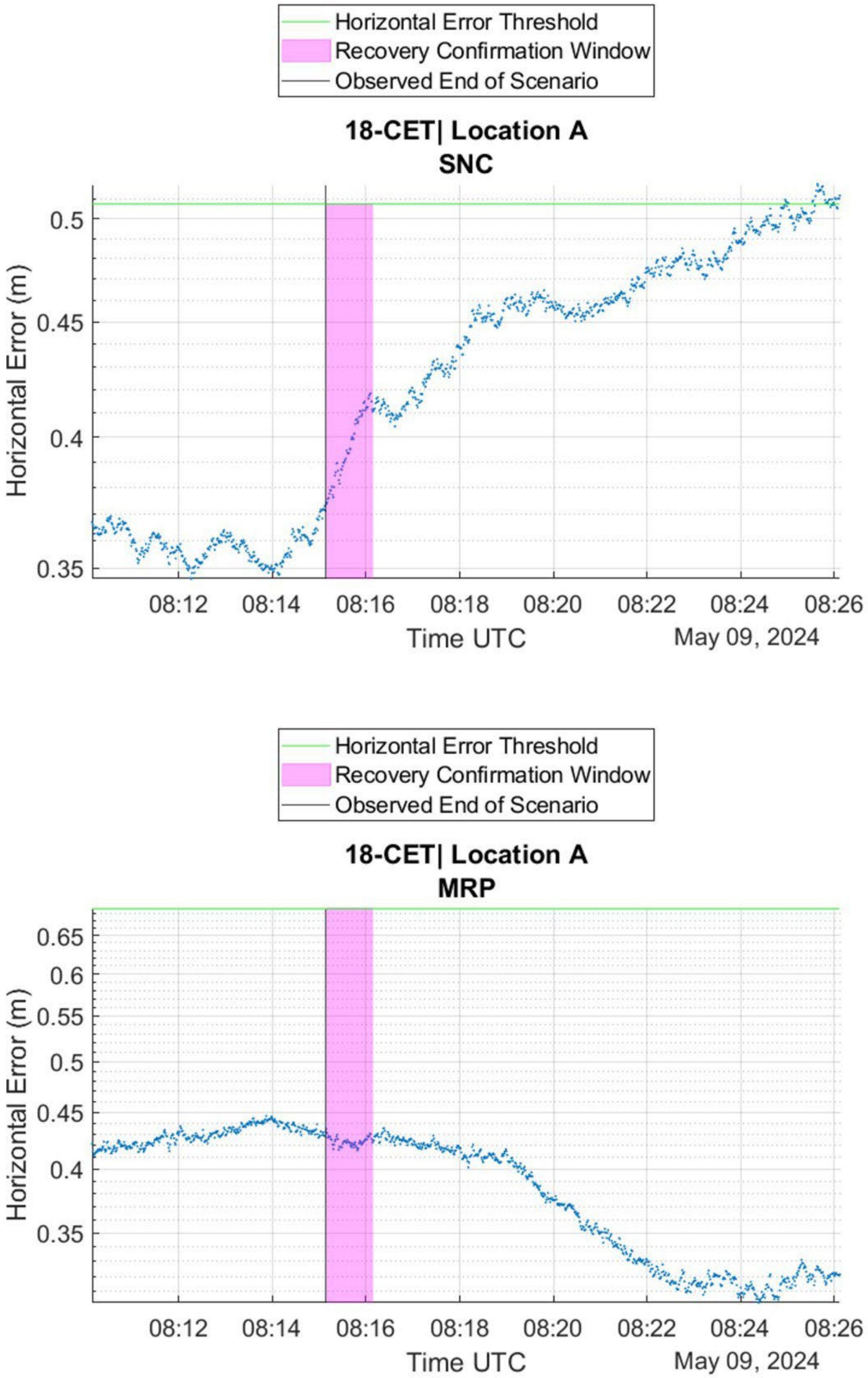


Figure 97. Static recovery analysis time series plots for scenario 18-CET

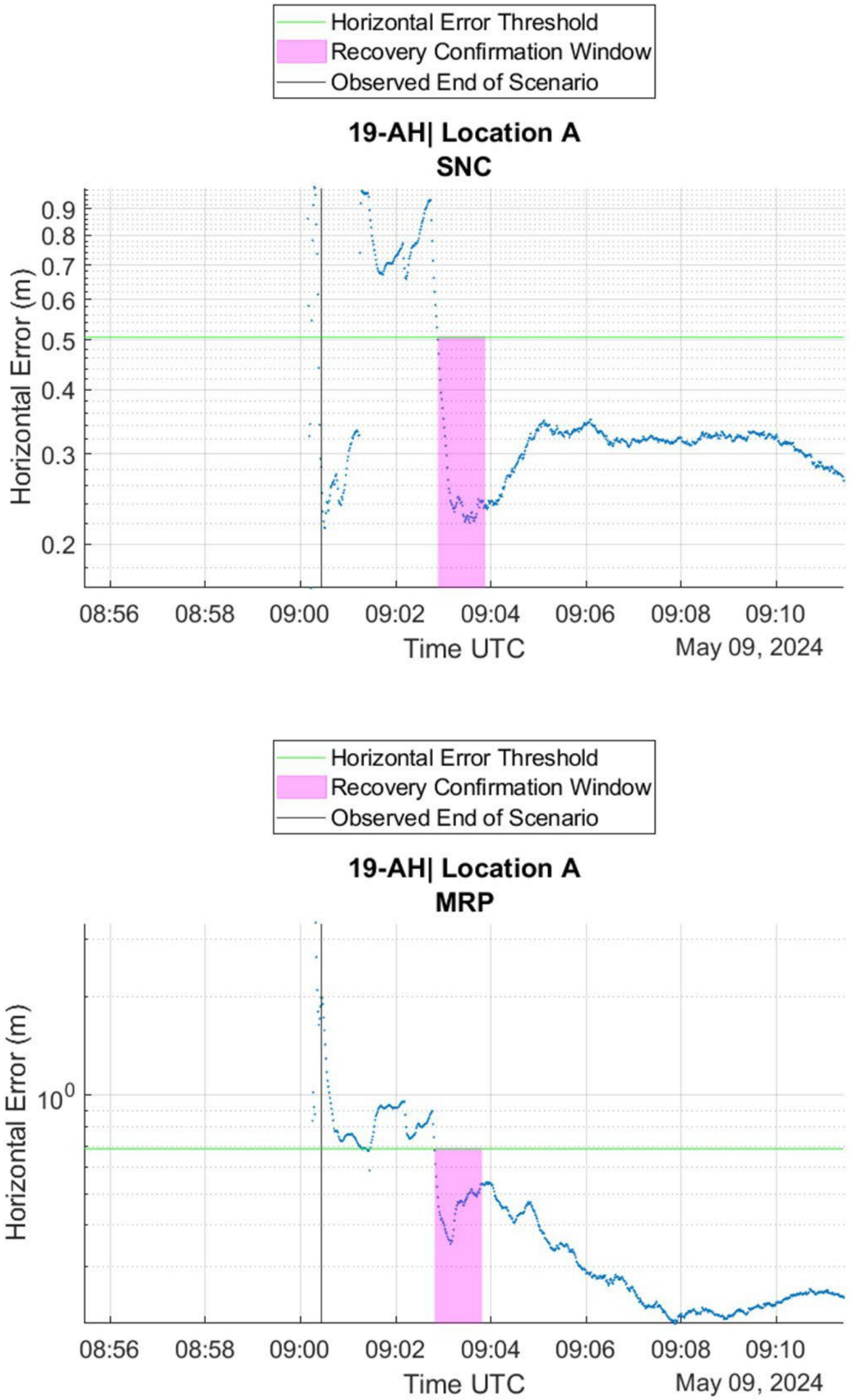


Figure 98. Static recovery analysis time series plots for scenario 19-AH

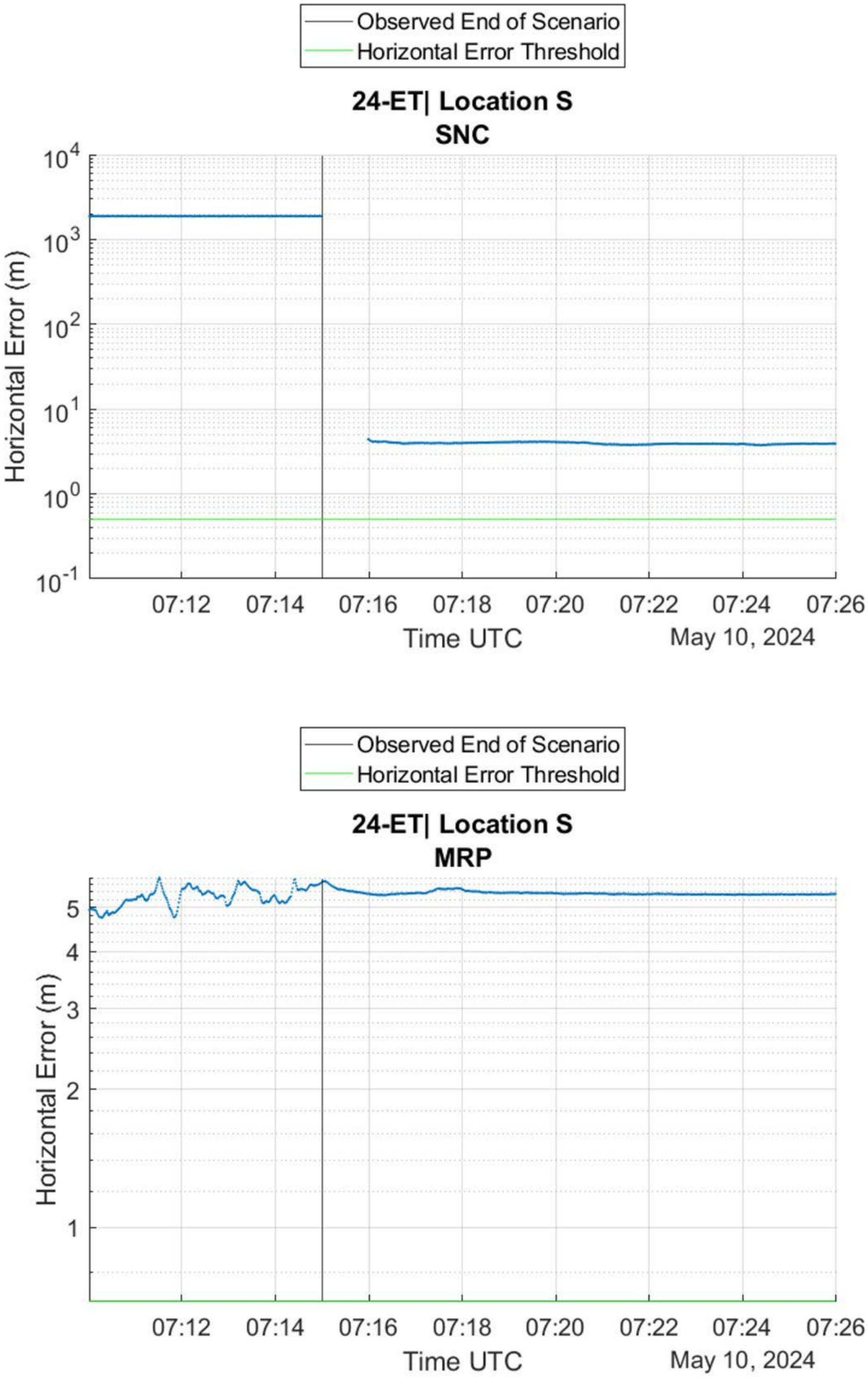
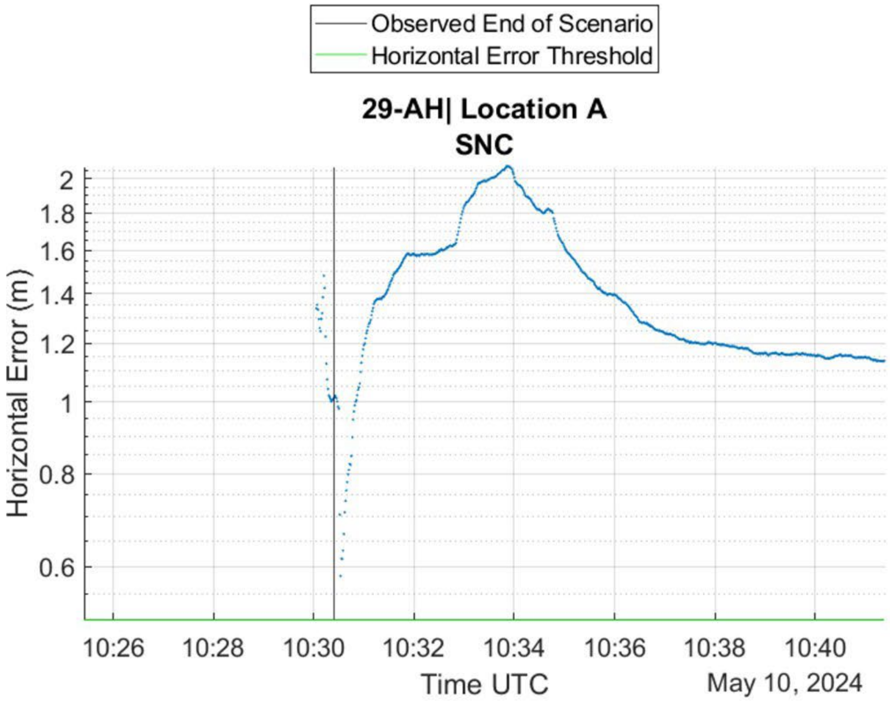


Figure 99. Static recovery analysis time series plots for scenario 24-ET



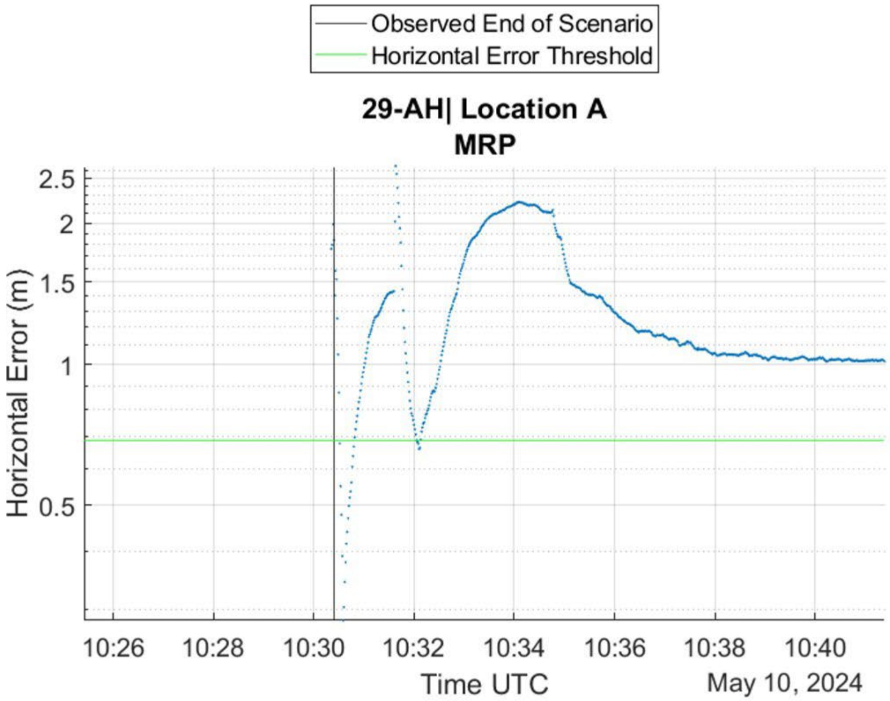
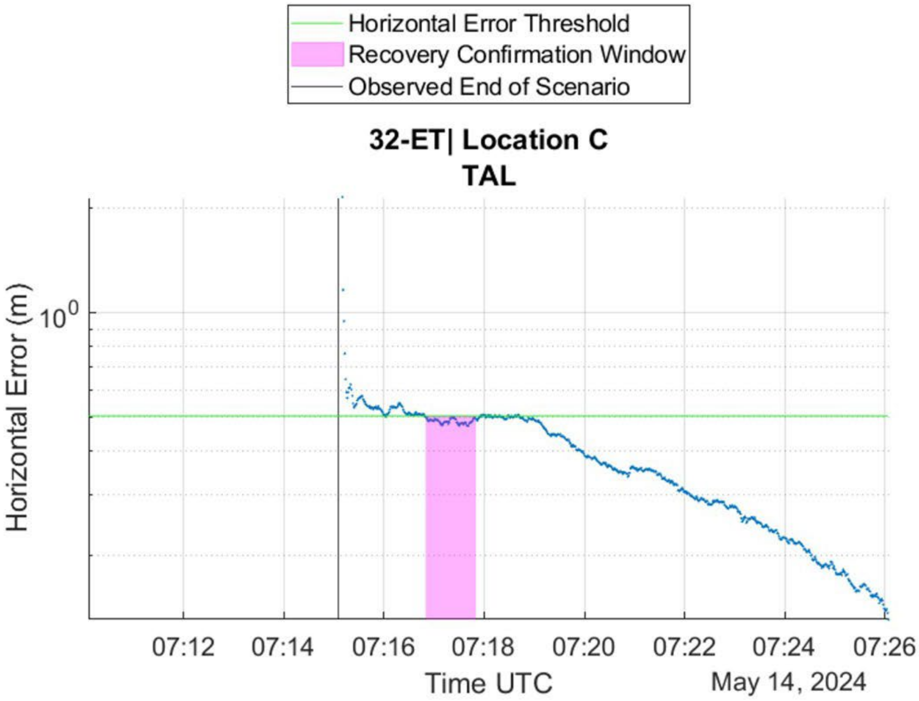


Figure 100. Static recovery analysis time series plots for scenario 29-AH



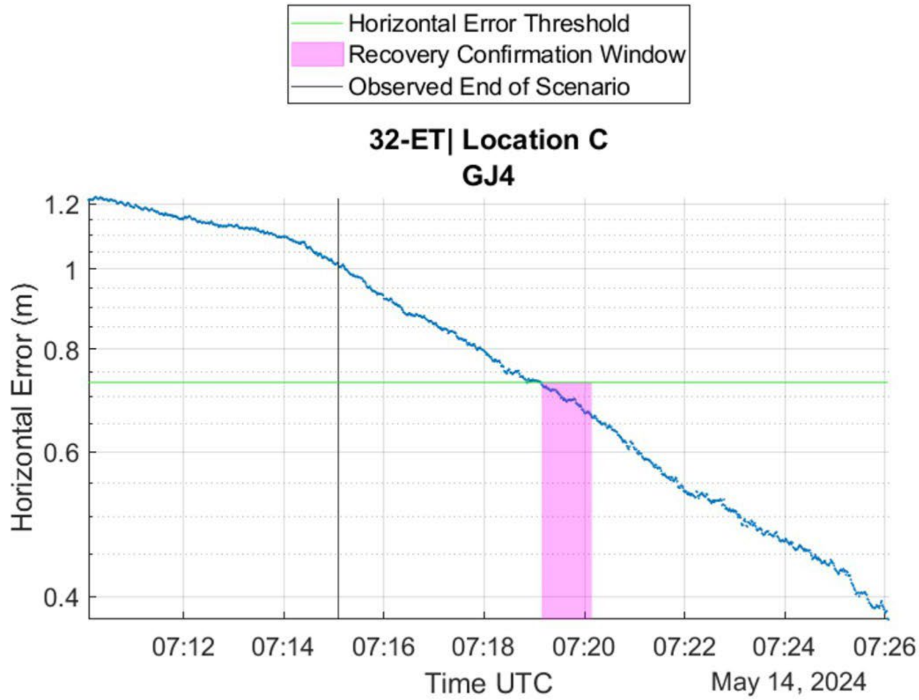
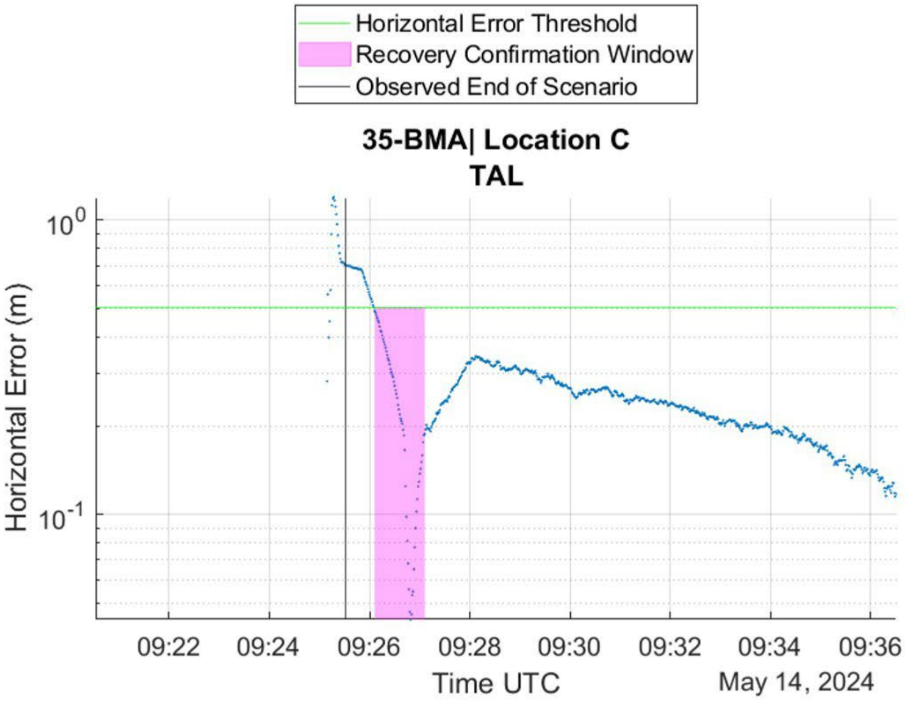


Figure 101. Static recovery analysis time series plots for scenario 32-ET



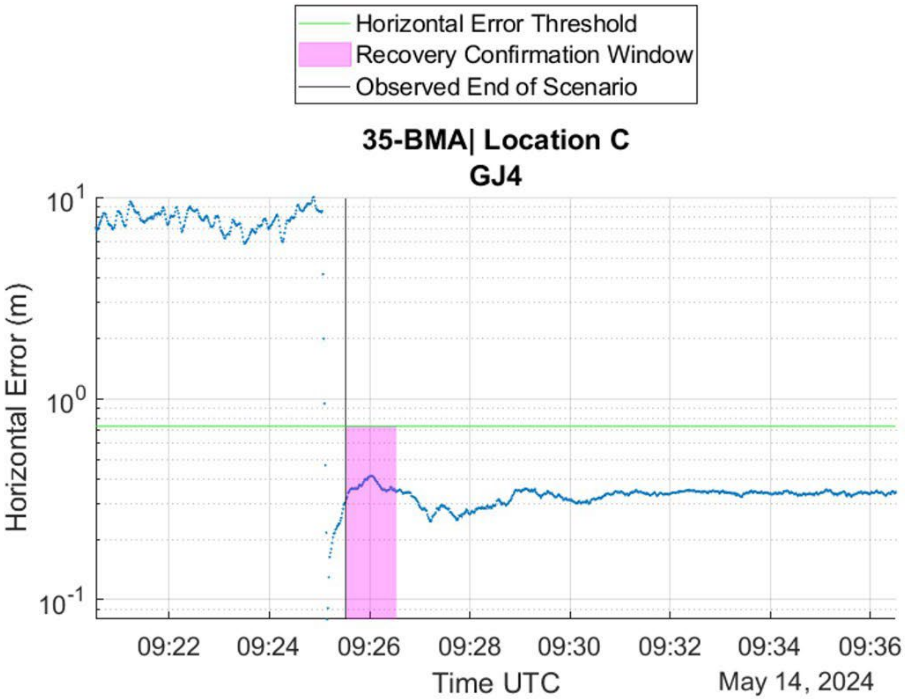
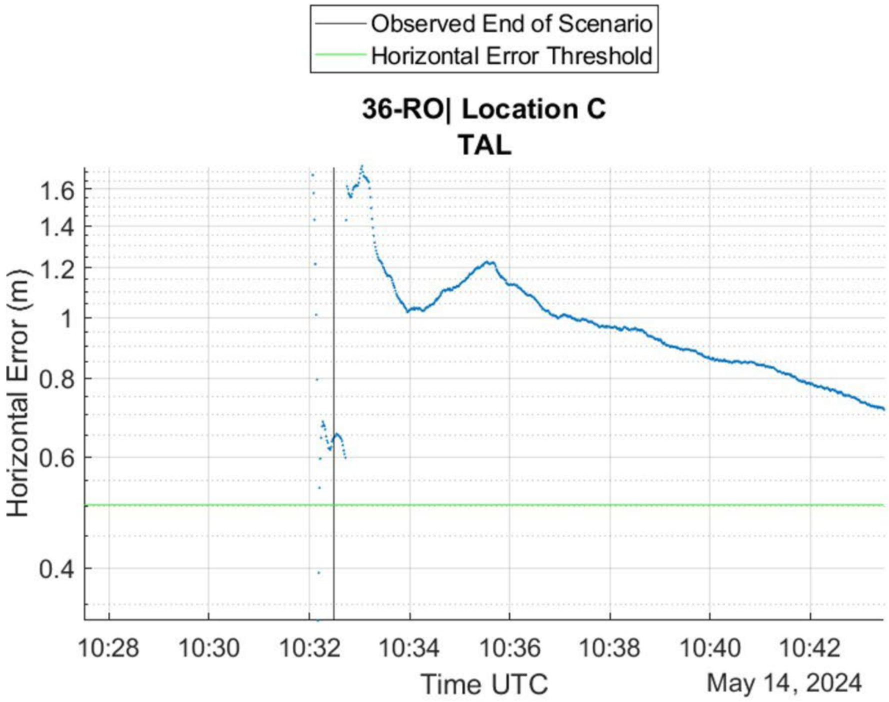


Figure 102. Static recovery analysis time series plots for scenario 35-BMA



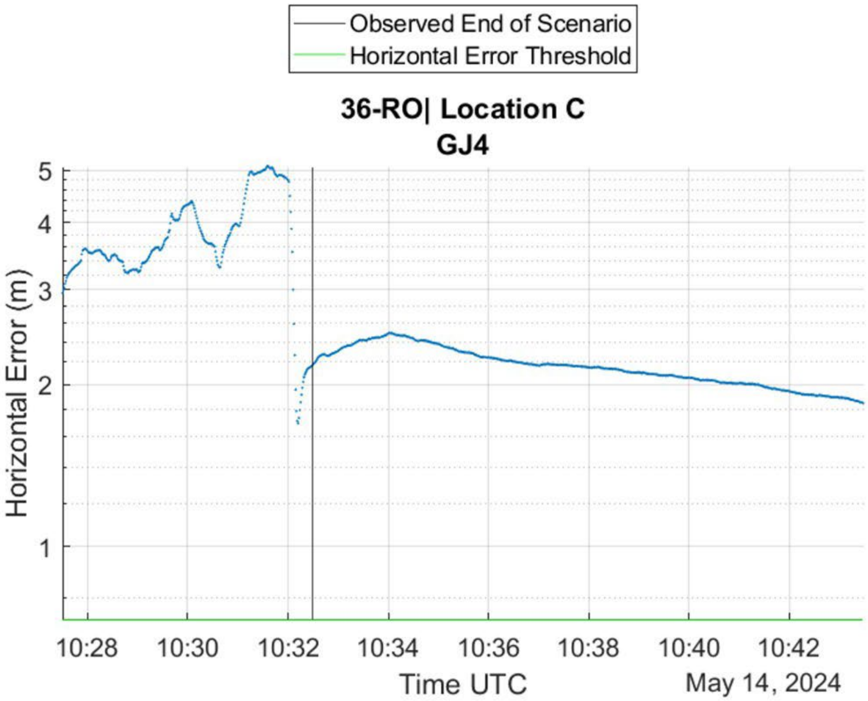


Figure 103. Static recovery analysis time series plots for scenario 36-RO

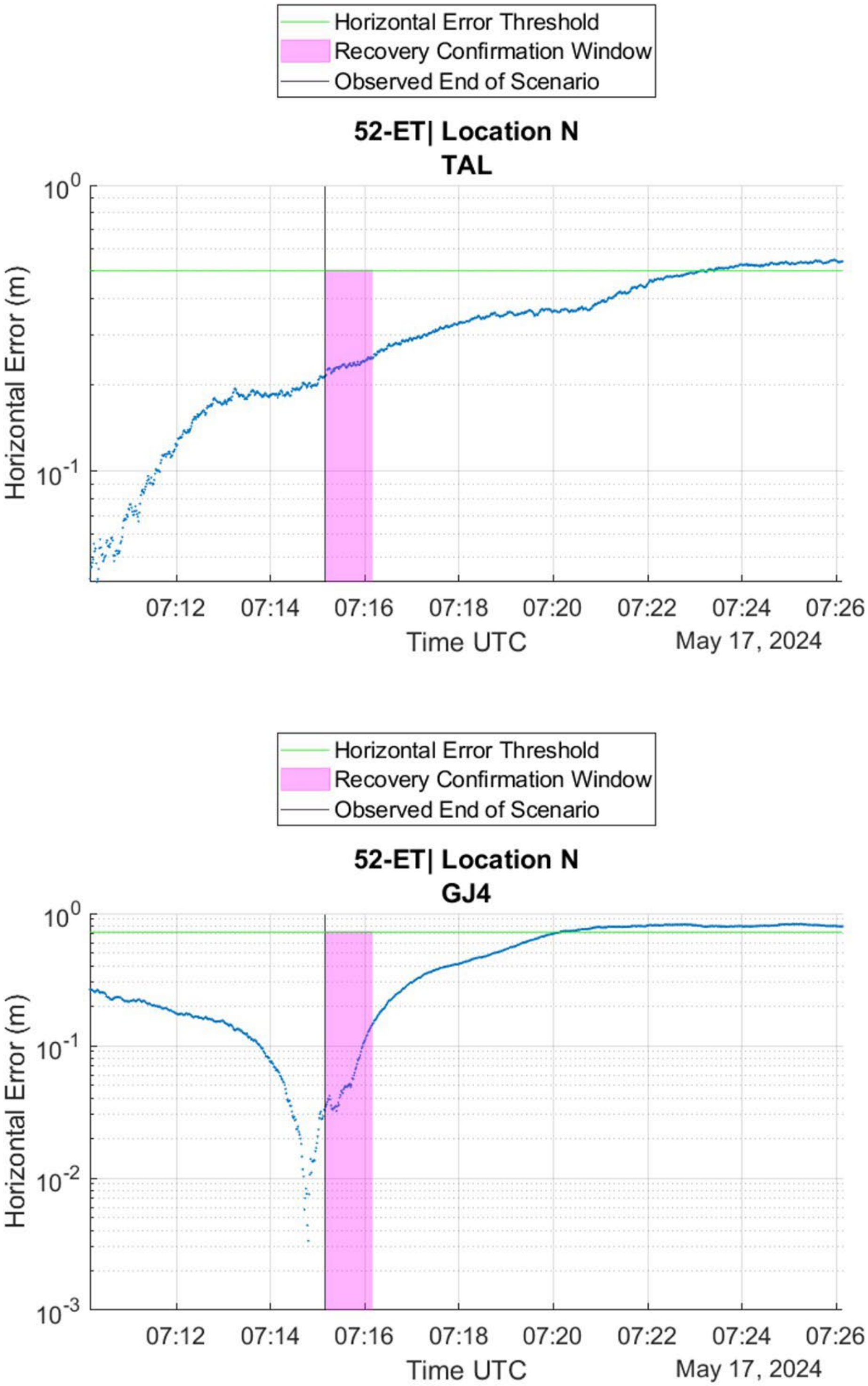


Figure 104. Static recovery analysis time series plots for scenario 52-ET

U.S. Department of Transportation
John A. Volpe National Transportation Systems Center
220 Binney St.
Cambridge, MA 02142-1093

617-494-2000
www.volpe.dot.gov

DOT-VNTSC- OST-25-05

U.S. Department of Transportation
Volpe Center

References

[1] 85 FR 9359, available at https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing

[2] About FRA | FRA (dot.gov), from https://railroads.dot.gov/about-fra/about-fra

[3] Program Offices Overview | FRA (dot.gov), from https://railroads.dot.gov/about-fra/program-offices/program-offices-overview

[4] Amtrak | FRA (dot.gov); from https://railroads.dot.gov/passenger-rail/amtrak/amtrak

[5] FRA 101: Getting to Know FRA. From https://railroads.dot.gov/sites/fra.dot.gov/files/2021-12/20210824-FRA101.pdf

[6] GPS Rail Applications. From https://www.gps.gov/applications/rail/

[7] "Denver GPS Interference Event After Action Report." Cybersecurity and Infrastructure Security Agency, National Risk Management Center, October 2022

[8] "GPS problems bedevil Denver RTD." https://www.gpsworld.com/gps-problems-bedevil-denver-light-rail/

[9] Railroad reports from https://www.ntsb.gov/investigations/AccidentReports/Pages/Reports.aspx

[10] "Beyond Positive Train Control: Using New and Emerging Technologies to Improve Rail Safety." NTSB News Release; 11-1-23. From https://www.ntsb.gov/news/press-releases/Pages/NR20231101.aspx .

[11] Image Source: NTSB Railroad Investigation Report RIR-22/14

[12] Federal Register: Positive Train Control Systems - A Rule by the Federal Railroad Administration on 07/27/2021. From https://www.federalregister.gov/documents/2021/07/27/2021-15544/positive-train-control-systems

[13] MxV Rail. From https://www.mxvrail.com/our-work/

[14] "Dead-reckoning keeps train positioning on track." International Railway Journal, March 2017. From https://www.railjournal.com/in_depth/dead-reckoning-keeps-train-positioning-on-track/

[15] Image Source: Wikipedia (Wikimedia Commons)

[16] Image Source: U.S. DOT / NTSB 2014

[17] Amtrak 2023 Host Railroad Report Card and FAQs. From https://www.amtrak.com/content/dam/projects/dotcom/english/public/documents/corporate/HostRailroadReports/Amtrak-2023-Host-Railroad-Report-Card.pdf

[18] "Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services," February 2021, Gaithersburg: National Institute of Standards and Technology, from https://doi.org/10.6028/NIST.IR.8323.

[19] The text in much of Section 2 highlights the rationale behind the adoption of NISTIR 8283, as described by NIST and adapted for the purposes of this report.

[20] "Cybersecurity Framework," National Institute of Standards and Technology, from https://www.nist.gov/cyberframework.

[21] "U.S. Department of Transportation Maritime Administration PNT Resiliency Pilot Program." March 2023.

[22] "Positive Train Control." Presentation to the Jun 2019 meeting of the National Space-Based PNTAB. From https://www.gps.gov/governance/advisory/meetings/2019-06/hayward-williams.pdf

[23] Caltrain PTC Implementation Plan (PTCIP). January 26, 2016.

[24] "USDOT Pilot Program: MARAD Phase II Final Report." Volpe Center, Dec. 2024.

[25] https://installations.militaryonesource.mil/in-depth-overview/u-s-army-garrison-white-sands-missile-range

[26] Wabtec product information from https://www.wabteccorp.com/digital-intelligence/signaling-and-train-control/train-control/golinc-precision-reference

[27] "AsteRx SB3 Pro+." Septentrio product data sheet.

[28] Amtrak drawing D-05-1355 Rev. E Sheet 1

[29] Tallysman product information from their web site at https://www.tallysman.com/product/?Antennas=true

[30] NovAtel product information from their web site at https://novatel.com/products/anti-jam-antenna-systems-gajt/

[31] "ICG and ITAR Update." Jeffrey Auerbach, briefing to U.S. PNTAB Meeting, November 16, 2022.

[32] "GPSS PNT Resiliency Discussion." Presentation by GPS Source to the Volpe Center, June 1, 2023.

[33] "Testing of Railway Assets Integrated Navigation (TRAIN) for the Alaska Railroad Corporation." Naval Information Warfare Center Pacific. July 20, 2020.

[34] FRA PTC web site, located at https://railroads.dot.gov/train-control/ptc/ptc-system-information

[35] "Low-Cost Multiple Sensor Inertial Measurement System for Locomotive Navigation." Report to the Transportation Research Board by ENCSO, Inc., July 1996.

[36] Image Source: https://www.amtrak.com/routes/acela-train.html

[37] AAR Spec M901, "Approved Draft Gear and Followers"

[38] Image Source: Teledyne Imaging

[39] "Digital Image Processing." Rafael C. Gonzalez and Richard E. Woods.

[40] "Ground Penetrating Radar (GPR) Technology Evaluation and Implementation." Federal Railroad Administration, May 2020.

[41] Image Source: Fugro

[42] Win, M. "Ultra-Wide Bandwidth: An Extreme Wireless Technique?" Laboratory for Information & Decision Systems (LIDS), Massachusetts Institute of Technology, Cambridge, MA 02139 USA. April 15, 2003. Accessible at https://www.media.mit.edu/events/2003-04-15-ec/win.pdf

[43] Discussions with Amtrak Sr. Technology Architecture Director, Eileen Reilly

[44] Source: https://gogeomatics.ca/ultra-wideband-pnt/

[45] Image Source: ENSCO

[46] "VEHICLE LAYOUT DOTX 216 ATIP INSPECTION CAR." ENSCO 29-Dec-2023. Dwg. no. SE-LOUT-0010842.

[47] "Amtrak Cities Sprinter | Electric locomotives from Siemens help power Amtrak and the Northeast's economy." Siemens Industry, Inc., Nov. 2014. https://assets.new.siemens.com/siemens/assets/api/uuid:d239ef45-cce3-4265-b670-79f536d5ad88/amtrak-electric-locomotives-case-study.pdf

[48] Source: ENSCO (TTC)

[49] Product Information from https://www.tualcom.com/gps-gnss-anti-jam-crpa/

[50] "ACS-64 LOCOMOTIVE." Amtrak 20-Feb-2024. Dwg. no. ROAD NOS: 600-670.

[51] Source: Amtrak (provided to Volpe).

[52] 132 Stat. 4276–4278, available at https://www.congress.gov/115/plaws/publ282/PLAW-115publ282.pdf

[53] Hansen, Andrew et al. "Complementary PNT and GPS Backup Technologies Demonstration Report." Prepared for the Office of the Assistant Secretary for Research and Technology, Department of Transportation (report DOT-VNTSC-20-07), January 2021,

[54] American Association of Railroads Standard S-9103.V1.0

[55] A Review on Technologies for Localisation and Navigation in Autonomous Railway Maintenance Systems," Sensors 2022, 22, 4185. https://doi.org/10.3390/s22114185

[56] Image Source: Volpe Center V-314 CTIL Simulator

[57] Image Source: "Positive Train Control Implementation Status, Issues, and Impacts." FRA Report to Congress, August 2012.

[58] Image Source: "Positive Train Control." FRA Briefing to National Space Based PNT Advisory Board, June 2019.

[59] "Positive Train Control: Engineering Basics and Lessons Learned." U.S. DOT FRA. FRA Program Delivery Conference, October 2015.

[60] From http://www.railway-technical.com/signalling/train-protection.html

[61] From https://www.bnsf.com/in-the-community/safety-and-security/positive-train-control.page